UNIVERZITET CRNE GORE

ELEKTROTEHNIČKI FAKULTET

G. Dragomir M. Stevanović dipl. inž.

Analiza uticaja kvantnih algoritama za faktorizaciju na savremene kriptografske sisteme i kvantna kriptografija

- MAGISTARSKI RAD -

Podgorica, 2017.

PODACI I INFORMACIJE O MAGISTRANTU	
Ime i prezime:	Dragomir Stevanović
Datum i mjesto rođenja:	20. 8.1968. Blažijevići, Srebrenica, BiH
Naziv završenog osnovnog studijskog programa i godina diplomiranja:	Elektrotehnički fakultet Podgorica, odsijek za elektroniku, 1993.
INFORMACIJE O MAGISTARSKOM RADU:	
Naziv postdiplomskog studija:	Elektrotehnički fakultet Podgorica, Poslijediplomske studije smjer telekomunikacije
Naslov rada:	Analiza uticaja kvantnih algoritama za faktorizaciju na savremene kriptografske sisteme i kvantna kriptografija
Fakultet na kojem je rad odbranjen:	Elektrotehnički fakultet Podgorica
UDK, OCJENA I ODBRANA MAGISTARSKOG RADA:	
Datum prijave magistarskog rada:	24. 5.2017.
Datum sjednice Vijeća univerzitetske jedinice na kojoj je prihvaćena tema:	6. 9.2017.
Komisija za ocjenu teme i podobnosti magistranta:	Prof. dr Igor Đurović, ETF Podgorica Prof. dr Slobodan Đukanović, ETF Podgorica Prof. dr David Kaljaj, PMF Podgorica
Mentor:	Prof. dr Igor Đurović
Komisija za ocjenu rada:	Prof. dr Slobodan Đukanović, ETF Podgorica Prof. dr Igor Đurović, ETF Podgorica Prof. dr David Kaljaj, PMF Podgorica
Komisija za odbranu rada:	Prof. dr Igor Đurović, ETF Podgorica Prof. dr Slobodan Đukanović, ETF Podgorica Prof. dr David Kaljaj, PMF Podgorica
Lektor:	Irena Pavlović, prof. crnogorskog- srp, hrv. i bos. jezika i književnosti
Datum odbrane:	28.12.2017.

Majci, koja nije prestala da vjeruje.

Gordani, Dušanu, Jeleni i Živku.

Sažetak

Informacija je u današnjem društvu jedan od najvažnijih resursa. Razmjena informacija, njihova obrada i upravljanje su najvažniji procesi u svakoj modernoj kompaniji ili instituciji. Stoga je razvoj sistema koji će obezbjediti povjerljivost, integritet, autentičnost i neporecivost tokom razmjene i čuvanja poruka, jedan od najvažnijih tehnoloških izazova današnjice. Savremeni kriptografski sistemi koji su razvijeni krajem 1970-ih godina, ponudili su tehnološke mehanizme koji obezbjeđuju sve ove potrebe. Na ovaj način, stvoreno je okruženje za razvoj novih industrijskih grana kao što su ePoslovanje (*eng. eBussiness*), eUprava (*eng. eGovernment*)... tzv. eServisi (*eng. eServices*). Sve ove nove industrijske grane zasnovane su na kriptografskim tehnologijama i veoma su osjetljive na bilo kakve prijetnje koje mogu imati uticaj na njihovu bezbjednost.

Sredinom 1980-ih godina pojavili su se prvi teorijski radovi o kvantnim kompjuterima. Kvantni kompjuteri nisu unaprijeđena verzija klasičnih kompjutera, već sasvim nova tehnologija. Ključna razlika između kvantnih i klasičnih kompjutera je eksponencijalno povećanje računskih sposobnosti. Prvi matematički algoritmi koji bi se mogli izvršavati na kvantnim kompjuterima i koji bi, koristeći njihove računske sposobnosti doveli do značajnog unaprijeđenja pojedinih procesa, patentirani su sredinom 1990-ih godina. Jedan od tih algoritama je algoritam kvantne faktorizacije Petera Shora, pomoću koga se faktorizacija velikih prirodnih brojeva na kvantnom kompjuteru može realizovati u polinomnom vremenu. U momentu patentiranja ovog algoritma, kvantni kompjuteri nisu postojali kao proizvod i uticaj ovog algoritma na savremene kriptografske sisteme je bio zanemariv. Razvoj kompjuterske tehnologije i pojava prvih kvantnih kompjutera su aktuelizovali potrebu za analizom uticaja algoritma kvantne faktorizacije na savremene kriptografske sisteme.

Na početku procesa analize u ovom radu, pojašnjena je matematička definicija faktorizacije i osnovne matematičke teoreme neophodne za razumijevanje različitih algoritama za faktorizaciju. Na osnovu poređenja teorijskih vremena neophodnih za faktorizaciju velikih prirodnih brojeva, korišćenjem nekoliko algoritama za faktorizaciju, sagledana je mogućnost donošenja relevantnih zaključaka. Izračunavanje teorijskih vremena faktorizacije realizovano je izradom programa za svaki analizirani algoritam respektivno. Konačni zaključak je da se, korišćenjem Shorovog algoritma kvantne faktorizacije na kvantnim kompjuterima, ogromni prirodni brojevi mogu faktorisati izuzetno brzo (u periodu od par stotina sekundi). S obzirom na to da je bezbjednost RSA algoritma asimetrične

kriptografije direktno povezana sa problemom faktorizacije velikih prirodnih brojeva, jasno je da je uticaj Shorovog algoritma kvantne faktorizacije na savremene kriptografske sisteme u ovom momentu izuzetno veliki.

Imajući u vidu značaj savremenih kriptografskih tehnologija na kompletno društvo, neophodno je započeti potragu za novim kriptografskim tehnologijama koje će eliminisati uticaj uočenih prijetnji. U tom smislu, posebna pažnja je posvećena upoznavanju sa novim tehnikama zaštite podataka, kvantnom kriptografijom i kvantnom distribucijom ključeva. Kombinovanjem tehnika kvantne kriptografije i Vernamovog One Time Pad kriptografskog Sistema (OTP), stvorena je mogućnost kreiranja bezuslovno bezbjednog kriptografskog sistema.

U ovoj tezi je ukazano na nove kompjuterske sisteme: kvantne kompjutere, na nove kriptografske tehnike – kvantnu kriptografiju, i na postojanje realnog uticaja Shorovog algoritma kvantne faktorizacije na bezbjednost savremenih kriptografskih sistema. Ukazivanje na prijetnje i narušavanje ukorjenjenog mišljenja da su savremeni kriptografski sistemi izuzetno bezbjedni, generisaće dodatne napore od strane naučne zajednice za razvojem novog, bezuslovno bezbjednog kriptografskog sistema. Ovo je izuzetno značajno za cijelo društvo, jer ne treba zaboraviti da je Troja pala zbog činjenice da Trojanci nisu bili svjesni prijetnje koja im dolazi od čuvenog „Trojanskog konja“.

Ključne riječi: *kvantni kompjuter, kvantna kriptografija, Shorov algoritam, kriptografija, kvantna faktorizacija.*

Abstract

Information is one of the most important resources nowdays. Information exchange, processing and management are the most important processes in every modern company or institution. Therefore, the development of a system that will ensure confidentiality, integrity, authenticity and nonrepudiation of messages during their exchange and storage is one of the most important current technological challenge. The modern cryptographic systems developed in the late 1970s offered technological mechanisms that satisfy all of these requirements. In this way, an environment has been created for the development of new industrial branches such as eBusiness, eGovernment... so-called eServices. All of these branches are based on cryptographic technologies and are very sensitive to any threats that could have an impact on their security.

In the mid-1980s, the first theoretical papers on quantum computers appeared. Quantum computers are not an upgraded version of classic computers but an entirely new technology. The key difference between quantum and classical computers is the exponential increase in computational capabilities. The first mathematical algorithms that could be performed on quantum computers, and which, using their computational capabilities, would lead to significant improvements in certain processes, were patented in the mid-1990s. One of these algorithms is the Peter Shor quantum factorization algorithm, by which factorization of large natural numbers on a quantum computer can be realized in polynomial time. At the moment of patenting this algorithm, quantum computers did not exist as a product and the impact of this algorithm on modern cryptographic systems was negligible. The development of computer technology and the emergence of the first quantum computers have actualized the need to analyze the impact of the quantum factorization algorithm on modern cryptographic systems.

At the beginning of the analysis process in this work, a mathematical definition of factorization and basic mathematical theorems necessary to understand the different factorization algorithmsare explained. Based on the comparison of theoretical times necessary for factoring large natural numbers using several factorization algorithms, the possibility of making relevant conclusions is considered. Calculation of theoretical factorization time was accomplished by creating a program for each analyzed algorithm respectively. The final conclusion is that using the Shor quantum factorization algorithm on quantum computers, we could factorize huge natural numbers extremely fast (in the period of

a couple of hundred seconds). Since security of the RSA algorithm (basic asymmetric cryptography algorithm) is directly related to the problem of factorization of large natural numbers, it is clear that the impact of Shor's quantum factorization algorithm on modern cryptographic systems at this moment is extremely large.

Having in mind the importance of modern cryptographic technologies to the whole of society, it is necessary to begin a search for new cryptographic technologies that will eliminate the impact of the perceived threats. In this regard, special attention is paid to getting acquainted with new data protection techniques, quantum cryptography and quantum key distribution. Combining the techniques of quantum cryptography and the Vernam's One Time Pad cryptographic system (OTP) has opened the possibility of creating an unconditionally secure cryptographic system.

The thesis identifies new computer systems - quantum computers, new cryptographic techniques - quantum cryptography, and the existence of a real impact of Shor's quantum factorization algorithm on the security of modern cryptographic systems. Pointing to threats and disturbing the accepted belief that modern cryptographic systems are extremely secure, will generate additional efforts by the scientific community to develop a new, unconditionally secure cryptographic systems. This is very important for our society and it should not be forgotten that Troy fell because of the fact that the Trojans were unaware of the threat that comes from the famous "Trojan Horse".

Key words: *quantum computer, quantum cryptography, Shor's algorithm, cryptography, quantum factorization.*

SADRŽAJ

1 Uvod

Bez ikakve sumnje možemo konstatovati da su elektronske komunikacije postale jedan od osnovnih stubova modernog društva i da njihov budući razvoj zahtijeva otkrivanje i implementaciju novih metoda i tehnika za zaštitu informacija tokom prenosa, ali i trajnog smještanja i čuvanja. Ovo je osnovni cilj nauke koja se zove kriptografija. Kriptografija potiče od grčkih riječi *κρυπτ΄ος* (skriveno ili tajno) i *γραφ΄η* (pisanje) i generalno se definiše kao nauka koja se bavi šifrovanjem (kriptovanjem) i dešifrovanjem (dekriptovanjem) poruka koristeći određene kodove, a u cilju obezbjeđivanja njihove povjerljivosti, integriteta, autentičnosti i neporecivosti (*eng. Confidentiality, Integrity, Authenticity–CIA*). Kriptoanaliza (*eng. Codebreaking*) je nauka koja se bavi razbijanjem šifrovanih poruka (kriptogram), kako bi se došlo do njihovog sadržaja. Kriptografija i kriptoanaliza zajedno čine kriptologiju (grčke riječi *κρυπτ΄ος* i *λ΄ογος*), nauku bezbjedne komunikacije.

Dugo vremena, kriptografija je uglavnom korišćena samo za zaštitu povjerljivih informacija. Razvoj savremenih kriptografskih sistema (asimetrična kriptografija ili kriptogafija javnog ključa) [4] i algoritama (RSA – **R**ivest, **S**hamir i **A**dleman) [5], krajem 1970-ih godina, stvorio je potpuno nove poslovne mogućnosti i doveo do razvoja veoma značajnih industrijskih grana kao što su ePoslovanje (*eng. eBussiness*), eUprava (*eng. eGovernment*)... tzv. eServisi (*eng. eServices*). Sve ove nove industrijske grane zasnovane su na novim kriptografskim tehnologijama i aplikacijama (npr. elektronski potpis, elektronski identitet, šifrovanje podataka...) i veoma su osjetljive na bilo kakve prijetnje koje mogu imati uticaj na njihovu bezbjednost.

Konstantni razvoj kompjuterske tehnologije i stalno povećanje gustine pakovanja logičkih kola, doveli su do realne mogućnosti početka proizvodnje i kvantnih kompjutera. Upotrebom kvantnih kompjutera u Shorovom algoritmu kvantne faktorizacije [16], može se napraviti faktorizacija velikih prirodnih brojeva u realnom vremenu. S obzirom na činjenicu da su svi moderni eServisi zasnovani na upotrebi tehnologija asimetrične kriptografije, čija pozdanost je bazirana na matematičkoj kompleksnosti faktorizacije velikih brojeva, uočena je mogućnost narušavanja bezbjednosti ovih sistema u slučaju upotrebe novih tehnologija. Stoga je, u ovom radu, napravljena analiza rizika za savremene kriptografske sisteme zbog razvoja kvantnih kompjutera i mogućnosti upotrebe Shorovog algoritama kvantne

faktorizacije [16], ali i upoznavanje novih tehnologija sa kojima bi se rizici mogli otkloniti u budućnosti.

U drugom poglavlju napravljen je pregled kriptografskih tehnika klasične kriptografije. Objašnjeni su osnovni koncepti simetrične i asimerične kriptografije i kombinacija obije tehnike u cilju dobijanja praktičnog kriptografskog sistema.

U trećem poglavlju objašnjeni su pojmovi kvantnih kompjutera i efekti kvantne mehanike koji su omogućili njihov nastanak. Razmatrane su razlike između klasičnih i kvantnih kompjutera i objašnjena osnovna razlika u dijelu teorije informacija, tj. pojam qubita. Pojašnjen je pojam kvantnih memorijskih registara i kvantni efekat superpozicije svih mogućih bit stanja. Imajući u vidu opisane kvantne efekte, došli smo do zaključka da kvantni kompjuteri nisu puko unapređenje klasičnih kompjutera u smislu poboljšanih performansi, već sasvim nova tehnologija koja nudi mogućnost eksponencijalnog povećanja računskih sposobnosti.

U četvrtom poglavlju pojašnjen je pojam faktorizacije i napravljena detaljna analiza trenutnog stanja nekoliko algoritama za faktorizaciju. U uvodnom dijelu poglavlja definisan je matematički aparat neophodan za razumjevanje pojma faktorizacije, ali i matematičke teoreme iz teorije brojeva neophodne za razumjevanje algoritama za faktorizaciju. Napravljeno je objašnjenje pojedinih algoritama vezanih za problem faktorizacije, kao što su: Euklidov algoritam, Eratostenovo sito polja brojeva, opšte sito polja brojeva i Shorov algoritam kvantne faktorizacije. Analizom vremena neophodnog za faktorizaciju velikih brojeva, koristeći različite algoritme, napravljeni su zaključci uticaja ovih algoritama na savremene kriptografske sisteme.

U petom poglavlju razmatrani su sistemi koji bi se mogli iskoristiti za otklanjanje rizika koji donose kvantni kompjuteri i Shorov algoritam kvantne faktorizacije, kao i mogućnosti za kreiranje bezuslovno bezbjednog kriptografskog sistema. U tom smislu, detaljno su opisani: Kvantna kriptografija i BB84 protokol za kvantnu distribuciju ključeva, pojam savršeno bezbjednog kriptografskog sistema i Vernamov One Time Pad (OTP) kriptografski sistem. Napravljen je prijedlog načina na koji bi se mogle kombinovati tehnike kvantne kriptografije i OTP kriptografskog sistema, u cilju dobijanja bezuslovno bezbjednog kriptografskog sistema.

U završnom (šestom) poglavlju, a na osnovu detaljne analize napravljene u prethodnim poglavljima, izneseno je mišljenje o trenutnom stanju savremenih kriptografskih sistema i

mogućnosti za prevazilaženje uočenih rizika. Iznesen je prijedlog mogućih pravaca za dodatna naučna istraživanja, koji može biti koristan potencijalnim istraživačima.

2 Klasična kriptografija

U ovom momentu, u oblasti kriptografije postoji podjela na sledeće osnovne kriptografske sisteme:

- **sistemi prikrivanja** od kojih su neki: pisanje poruka nevidljivim mastilom, sakrivanje poruka u raznim tekstualnim člancima (npr. novinski članci, knjige...), sakrivanje poruka u slikama (steganografija). Osnovna karakteristika ovih kriptografskih sistema je da je poruka u nešifrovanoj formi sakrivena od neprijatelja, na način da on nije svijestan postojanja poruke. Jedan od najstarijih primjera upotreba ovih sistema je brijanje glave kuriru, ispis poruke na glavi, čekanje da kosa naraste, i slanje kurira na odredište;
- **pouzdani sistemi** od kojih su neki: govor unazad, ili zamjena slova u alfabetu sa određenim znakovima. Osnovna karakteristika ovih sistema je da je potrebna posebna oprema za dobijanje originalne poruke, ali da semantika same poruke i njene osnovne karakteristike nisu promjenjene ili sakrivene. Ovo su bili veoma popularni sistemi zaštite podataka u istoriji, a, samim tim, intrigantni i za mnoge pisce koji su se bavili temama kriminala. Jedno od najstarijih djela u kome je ovaj metod upotrebljen za zaštitu podataka je djelo Artura Konana Doyla „The Adventure of the Dancing Men“ [1]. U djelu je opisan način bezbjedne komunikacije u kome je svako slovo engleskog alfabeta zamjenjeno sa odgovarajućim crtežom koji liči na razne plesne položaje, stoga je i naziv dijela logičan („Avanture plesača“);
- „**stvarno” bezbjedni sistemi** čija je osnovna karakteristika da je sadržaj poruke sakriven koristeći razne kodove, kriptografske algoritme, ili druge metode, a samo postojanje poruke nije sakriveno. Osnovna pretpostavka ovih sistema je da neprijatelj ima svu neophodnu tehnologiju potrebnu za presretanje i snimanje poruka tokom njihovog prenosa između različitih strana i neograničene tehničke mogućnosti u dijelu analize i dešifrovanja presretnutih poruka. Čak i pod ovim uslovima, cilj je da se do sadržaja originalne poruke ne može doći.

U ovom radu bavićemo se samo kriptografski bezbjednim sistemima, s obzirom na to da su kriptografski sistemi prikrivanja generalno vezani za psihološke metode zaštite, a kriptografski pouzdani sistemi vezani za tehnološke metode zaštite.

Osnovni zahtijevi koji se postavljaju pred određeni kriptografski sistem, u dijelu bezbjedne komunikacije preko javnog kanala koji nije pouzdan, su:

- da obezbijedi privatnost komunikacije (*eng. Privacy*). Ovo znači da sistem mora da spriječi da neovlašćene osobe dođu u posjed povjerljivih informacija koje se razmjenjuju;
- da obezbijedi autentifikaciju osoba koje učestvuju u komunikaciji (*eng. Authentication*). Ovo znači da sistem mora da obezbijedi pouzdanu autentifikaciju osoba, tako da neovlašćene osobe ne mogu da šalju ili primaju informacije;
- da obezbijedi integritet komunikacije (*eng. Integrity*). Ovo znači da sistem mora da obezbijedi mehanizme pomoću kojih se, na pouzdan način, može provjeriti da li je došlo do promjene informacija tokom prenosa.

U klasičnoj kriptografiji postoji podijela na dva osnovna kriptografska sistema:

- Simetrična kriptografija, ili kriptografija tajnog ključa;
- Asimetrična kriptografija, ili kriptografija javnog ključa.

2.1 Simetrična kriptografija

Simetričnu kriptografiju, u formi u kojoj je danas znamo, definisao je Claude Shannon, čuveni američki matematičar, elektroinženjer i kriptograf (poznat kao otac informatike), u svom djelu iz 1949. godine [3].

Simetrični kriptografski sistem je jednoparametarska familija $\{T_K\}_{K\in|K|}$ invertibilnih transformacija

$$T_K: \{M\} \to \{E\}$$

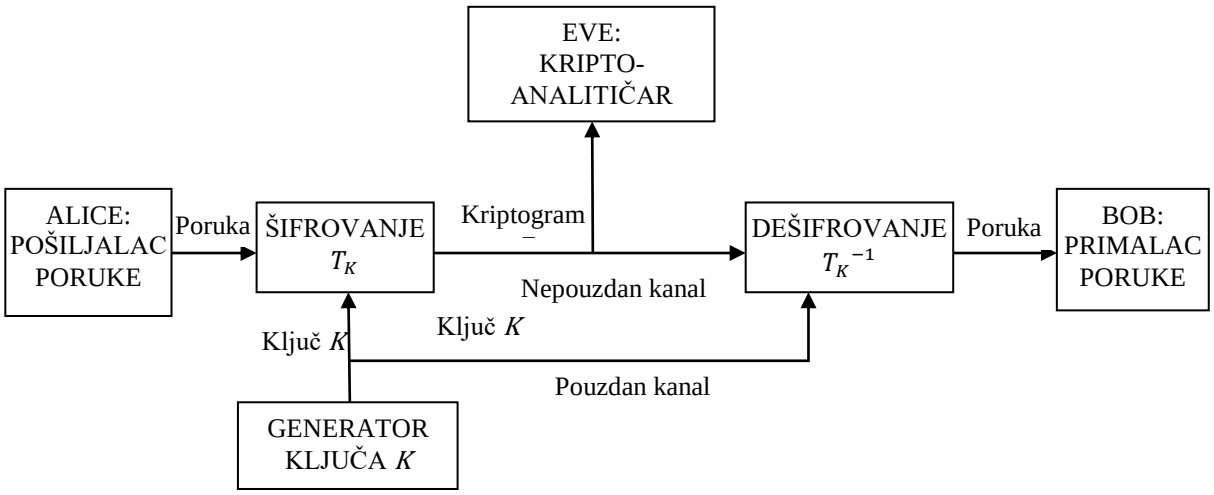
iz skupa $\{M\}$ nešifrovanih poruka u skup $\{E\}$ šifrovanih poruka. Parametar K se naziva ključ i on može biti izabran iz konačnog skupa $\{K\}$ koji se naziva skup ključeva (*eng. keyspace*).

Osnovno pravilo koje određeni kriptografski sistem treba da zadovolji je da kvalitet šifrovanog teksta (kriptograma) ne smije da zavisi od algoritma za šifrovanje koji se koristi,

odnosno transformacije $T_K(M)$, već samo od osobina ključa K. Na ovaj način, mijenjajući ključ K, može da se poveća bezbjednost kriptografskog sistema i, na taj način, spriječi proboj bezbjedne komunikacije i dospijeće povjerljivih informacija u neželjene ruke. Promjena osobina ključa K može da se realizuje na veoma jednostavan način.

Shannon je na sistematski način definisao osnovne pojmove vezane za razmjenu poruka na bezbjedan način, kao i sam proces šifrovanja i dešifrovanja poruka.

Na slici 1 je prikazan opšti komunikacioni sistem kod simetrične kriptografije.



Slika 1: *Šematski prikaz simetričnog kriptografskog komunikacionog sistema*

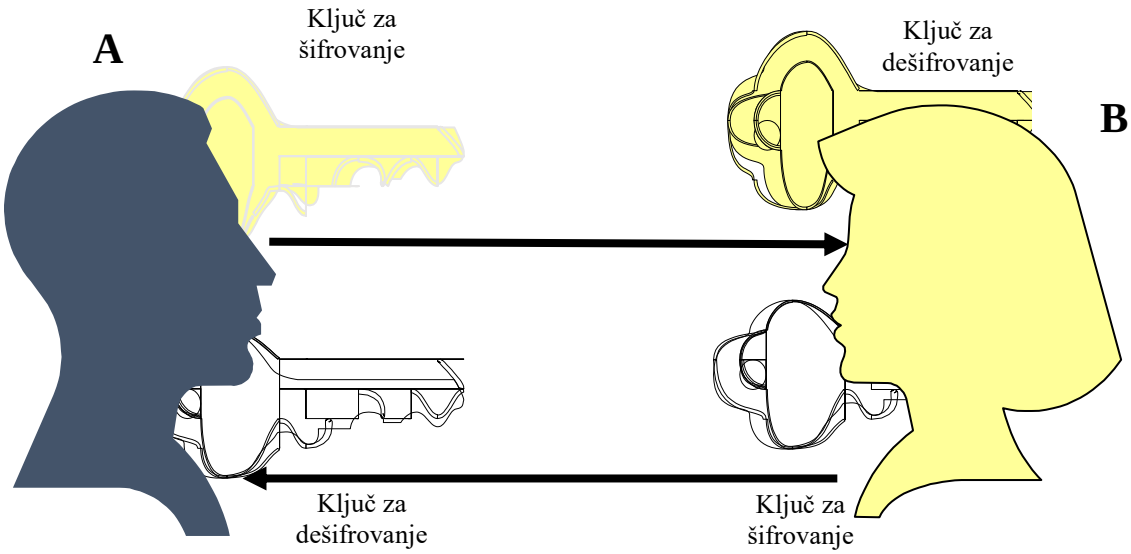
Osnovni pojmovi:

- `Alice, Bob,` i `Eve` su generičke oznake učesnika u bezbjednoj komunikaciji, i to: `Alice` je izvor poruke tj. pošiljalac poruke, `Bob` je primalac poruke, `Eve` je neprijateljski kriptoanalitičar čiji je jedini cilj da dođe do povjerljivih podataka i za to ima neograničena finansijska i analitička sredstva;
- `Poruka` (*eng. Plaintext*) je poruka koja nije šifrovana, ali je pripremljena na odgovarajući način za šifrovanje;
- `Generator ključa` je sistem koji na pouzdan način generiše ključ K određenih karakteristika;
- `Ključ` K je neophodni podatak za šifrovanje poruke;
- `Šifrovanje` (T_K) je transformacija koja, koristeći ključ K i određeni algoritam, transformiše poruku iz čitljive u nečitljivu formu;
- `Kriptogram` je poruka u nečitljivoj formi, tj. šifrovana poruka: $E = T_K(M)$;

- `Dešifrovanje` (T_K^{-1}) je transformacija koja, koristeći ključ K i određeni algoritam, transformiše poruku iz nečitljive u čitljivu formu: $M = T_K^{-1}(E) = T_K^{-1}(T_K(M))$;
- `Pouzdan kanal` je metod za prenošenje male količine povjerljivih podataka, kao što je ključ K. Pouzdan kanal ne može biti korišćen za prenos povjerljive poruke M , zbog malog kapaciteta ili visokih kašnjenja;
- `Nepouzdan kanal` je metod za prenošenje šifrovane poruke (kriptograma) i ovom kanalu pristup imaju neovlašćeni učesnici u komunikaciji, kao što je `Eve` – kriptoanalitičar.

Najvažnija osobina ovog kriptografskog sistema je da se za šifrovanje i dešifrovanje poruka koristi isti ključ. Zbog toga je i naziv ovog kriptografskog sistema simetrična kriptografija, ili kriptografija tajnog ključa.

Na slici 2 je prikazano korišćenje tajnog ključa u procesu komunikacije kod simetrične kriptografije.



Slika 2: *Šematski prikaz korišćenja tajnog ključa kod simetrične kriptografije*

Kada osoba A želi da pošalje povjerljivu poruku osobi B, ona koristi ključ K za šifrovanje poruke. Kada osoba B želi da dešifruje poruku, ona koristi isti ključ K sa kojim je osoba A šifrovala poruku. Ista je situacija i kada osoba B želi da pošalje povjerljivu poruku osobi A, sa tim što bi za ovu situaciju mogli da koristimo drugi ključ za šifrovanje/dešifrovanje, što se u praksi veoma rijetko primjenjuje. Bez obzira na praksu, zbog kompletnosti, na slici 2 je

prikazana situacija kada se za povjerljivu komunikaciju od osobe B ka osobi A koristi drugi ključ.

S obzirom na to da se isti ključ koristi za šifrovanje i dešifrovanje podataka, posebna pažnja se mora posvetiti čuvanju ovog ključa.

Tokom vremena su razvijeni mnogi algoritmi za šifrovanje/dešifrovanje podataka koji se primjenjuju u simetričnoj kriptografiji. Tema ovog rada nije analiza pojedinačnih algoritama za šifrovanje/dešifrovanje, već navodimo samo neke od njih kao referencu: LUCIFER, DES, 3DES, FEAL, IDEA, RC4, RC5, SKIPJACK, BLOWFISH, TWOFISH, AES (RIJNDAEL) AES [7].

Jedna od veoma važnih osobina simetrične kriptografije su dobre performanse. Ovo znači da je moguće šifrovati velike količine podataka u relativno kratkom roku.

Problemi kod simetrične kriptografije su:

- distribucija tajnog ključa (*eng. Key Distribution Problem*). Tajni ključ mora biti distribuiran na bezbjedan način i prije početka komunikacije. Ovo je veoma važan problem, jer se najčešći proboji u simetričnoj kriptografiji zasnivaju na obezbjeđivanju tajnog ključa;
- veliki broj ključeva koji je neophodan za komunikaciju više osoba na bezbjedan način. Potreban je različit tajni ključ za svakog partnera sa kojim želimo da ostvarimo bezbjednu komunikaciju. U situaciji gdje imamo n osoba, gdje svaka treba da komunicira sa svakom osobom na bezbjedan način, ukupan broj ključeva koje je potrebno obezbjediti je:

  $$\text{Ukupan broj ključeva} = \frac{n(n-1)}{2}$$

  Za 1000 osoba, ukupan broj ključeva je čak 499500. Ovo je ogroman broj ključeva koje je praktično nemoguće čuvati na pouzdan način i ovo je važan problem, koji praktično onemogućava upotrebu simetrične kriptografije za bezbjednu komunikaciju velikog broja ljudi;
- nemoguće je provjeriti koja strana je kreirala šifrovanu poruku, s obzirom na to da obije strane koriste isti ključ i za šifrovanje i za dešifrovanje podataka. Zbog ovog problema nije moguće autentifikovati učesnike u komunikaciji.

2.2 Asimetrična kriptografija

Koncept asimetrične kriptografije prvi su teorijski definisali Whitfield Diffie, Martin Helman i Ralph Merkle u svom radu iz 1976. godine [4].

Asimetrični kriptografski sistem je par familija $\{E_K\}_{K\in|K|}$ i $\{D_K\}_{K\in|K|}$ različitih algoritama predstavljenih invertibilnim transformacijama

$$E_K: \{M\} \rightarrow \{M\}$$

$$D_K: \{M\} \rightarrow \{M\}$$

Na konačnom skupu poruka $\{M\}$ takav da su zadovoljeni sljedeći uslovi:

1. Za svako $K \in \{K\}$, E_K je inverzna transformacija od D_K,
2. Za svako $K \in \{K\}$ i $M \in \{M\}$, algoritmi E_K i D_K su jednostavni za računanje,
3. Za skoro svako $K \in \{K\}$, svaki algoritam koji bi bio ekvivalentan sa D_K je računski neisplativo tražiti na osnovu E_K,
4. Za svako $K \in \{K\}$, isplativo je izračunati inverzne parove E_K i D_K na osnovu K.

Zahvaljujući trećem uslovu, korisnički javni ključ za šifrovanje E_K moguće je javno objaviti bez kompromitovanja bezbjednosti njegovog privatnog ključa za dešifrovanje D_K. Zbog ovoga, kriptografski sistem je podijeljen na dva dijela: familije transformacija za šifrovanje i familije transformacija za dešifrovanje i to na takav način, da je za jednog člana familije neisplativo naći odgovarajući član druge familije.

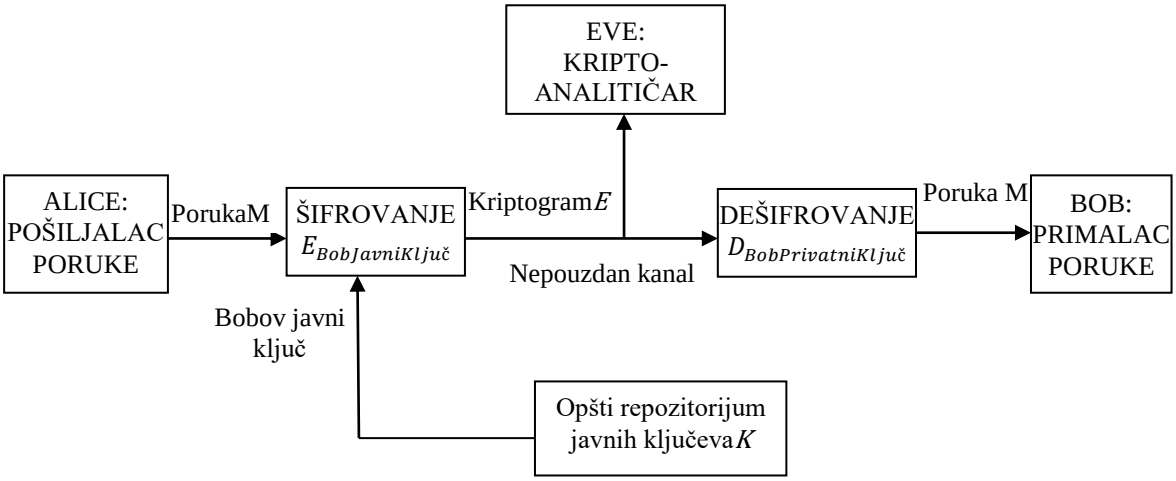
Potraga za neprobojnim kriptografskim sistemom je jedan od najstarijih ciljeva kriptografije. Mnogo puta u istoriji, pojedini sistemi su proglašavani za neprobojne, a tokom vremena se to pokazalo netačnim. Činjenica je da bezbjednost većine kriptografskih sistema počiva u računskoj kompleksnosti koja stoji pred kriptoanalitičarom, koji pokušava da otkrije nešifrovani tekst, bez poznavanja ključa koji je korišćen za šifrovanje. Zbog toga se u definicijama asimetrične kriptografije koristi termin računski neisplativo, kada se želi naglasiti da je određeni zadatak skoro nemoguće realizovati sa postojećim znanjima i tehnologijama. Za određeni zadatak se kaže da je računski neisplativ, ako se cijena njegove realizacije mjeri bilo iznosom memorije, bilo iznosom neophodnog vremena i ako su ove vrijednosti konačne, ali nevjerovatno velike. Na ovaj način imamo korektne definicije, jer se ostavlja mogućnost da će otkrića novih algoritama, ili nova unapređenja tehnologije dovesti

do toga da je dešifrovanje poruka moguće realizovati u budućnosti i bez poznavanja ključa koji je korišćen za šifrovanje.

Kriptografski sistemi koji su bezbjedni u odnosu na računsku isplativnost jednog kriptoanalitičara, ali, koji mogu podleći napadu koji bi koristio neograničene računske mogućnosti, nazivaju se *računski bezbjedni*. Kriptografski sistemi koji su otporni na napad bilo kog kriptoanalitičara, čak i onog koji na raspolaganju ima neograničene računske i finansijske resurse, nazivaju se *bezuslovno bezbjedni*.

Sistem asimetrične kriptografije spada u računski bezbjedan sistem. Dobra osobina ovog sistema je što se promjenom dužine ključa može uticati na njegovu bezbjednost. Za računski bezbjedne sisteme koji zahtijevaju 2^{100} tj. 10^{30} operacija da bi se došlo do povjerljivih informacija, smatra se da su skoro bezuslovno bezbjedni. Razlog tome je što je ukupno vrijeme potrebno da bi se došlo do povjerljivih informacija čak i u situaciji gdje bi se obrađivalo više miliona operacija u sekundi, višestruko veće od starosti univerzuma.

Na slici 3 je prikazan opšti komunikacioni sistem kod asimetrične kriptografije.



Slika 3: *Šematski prikaz asimetričnog kriptografskog komunikacionog sistema*

Osnovni pojmovi:

- `Alice`, `Bob`, i `Eve` su generičke oznake učesnika u bezbjednoj komunikaciji, i to: `Alice` je izvor poruke tj. pošiljalac poruke, `Bob` je primalac poruke, `Eve` je neprijateljski kriptoanalitičar čiji je jedini cilj da dođe do povjerljivih podataka i za to ima neograničena finansijska i analitička sredstva;

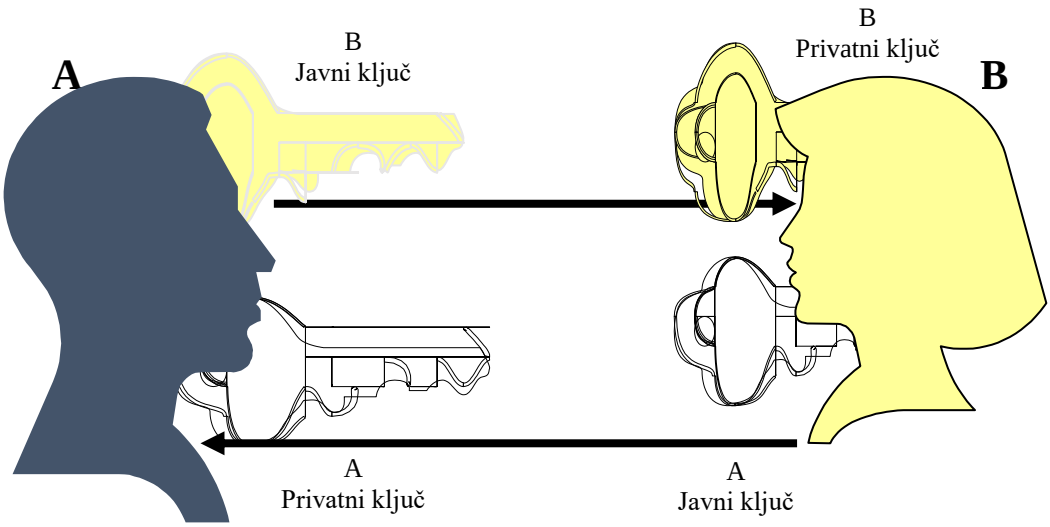
- `Poruka` (*eng. Plaintext*) je poruka koja nije šifrovana, ali je pripremljena na odgovarajući način za šifrovanje;
- `Opšti repozitorijum javnih ključeva` je dio sistema kome svaki učesnik u bezbjednoj komunikaciji ima pristup, tako da može da nađe javni ključ primaoca poruke kome želi da pošalje povjerljive podatke;
- `Bobov javni ključ` je neophodni podatak za šifrovanje poruke;
- `Bobov privatni ključ` je neophodni podatak za dešifrovanje poruke;
- `Šifrovanje` ($E_{BobJavniKljuč}$) je transformacija koja, koristeći `Bobov javni ključ` i određeni algoritam, transformiše poruku iz čitljive u nečitljivu formu;
- `Kriptogram` je poruka u nečitljivoj formi, tj. šifrovana poruka: $E = E_{BobovJavniKljuč}(M)$;
- `Dešifrovanje` ($D_{BobPrivatniKljuč}$) je transformacija koja, koristeći `Bobov privatni ključ` i određeni algoritam, transformiše poruku iz nečitljive u čitljivu formu:
  $M = D_{BobPrivatniKljuč}(E) = D_{BobPrivatniKljuč}(E_{BobJavniKljuč}(M))$;
- `Nepouzdan kanal` je metod za prenošenje šifrovane poruke (kriptograma) i ovom kanalu pristup imaju neovlašćeni učesnici u komunikaciji kao što je `Eve` – kriptoanalitičar.

Najvažnija osobina ovog kriptografskog sistema je da se za šifrovanje i dešifrovanje poruka koriste različiti ključevi. Ovi ključevi su povezani i jedan je javni, a drugi privatni ključ. Zbog toga je i naziv ovog kriptografskog sistema asimetrična kriptografija, ili kriptografija javnog ključa.

Osnovni principi upotrebe javnog i privatnog (tajnog) ključa su sljedeći:

- podaci se šifruju javnim ključem primaoca podataka;
- dešifrovanje podataka se obavlja odgovarajućim privatnim ključem primaoca podataka;
- kada se javni ključ koristi za šifrovanje podataka, podaci se mogu dešifrovati samo sa odgovarajućim privatnim ključem i obrnuto;
- potrebno je enormno vrijeme i snaga kompjutera da bi se na osnovu javnog ključa generisao privatni ključ.

Na slici 4 je prikazano korišćenje javnog i privatnog ključa u procesu komunikacije kod asimetrične kriptografije.



Slika 4: *Šematski prikaz korišćenja javnog i privatnog (tajnog) ključa kod asimetrične kriptografije*

Kada osoba A želi da pošalje povjerljivu poruku osobi B, ona koristi javni ključ osobe B za šifrovanje poruke. Kada osoba B želi da dešifruje poruku, ona koristi svoj privatni ključ, koji je povezan sa njenim javnim ključem i jedino ovim ključem mogu da se dešifruju poruke koje su šifrovane javnim ključem osobe B. Analogna procedura važi kad osoba B želi da pošalje poverljivu informaciju osobi A. Na ovaj način za bezbjednu komunikaciju između dvije osobe potrebna su ukupno, dva javna i dva privatna ključa.

Kod asimetrične kriptografije, neophodno je posebnu pažnju posvetiti čuvanju privatnog ključa, s obzirom na to da se njim vrši dešifrovanje poruka, dok javni ključ može da se distribuira slobodno, bez preduzimanja bilo kakvih bezbjedonosnih mjera.

Prvi algoritam koji je omogućio praktičnu upotrebu asimetrične kriptografije je RSA algoritam (Rivest, Shamir, Adleman) koji je objavljen 1976. godine [5]. Tokom vremena su razvijeni i drugi algoritmi, ali je RSA algoritam ostao osnovni algoritam asimetrične kriptografije i sa njim je praktično omogućen razvoj novih aplikacija kao što su digitalni potpis, autentifikacija osoba i mnoge druge komercijalne aplikacije.

Na osnovu svega navedenog, jasno je da su sa asimetričnom kriptografijom riješeni svi bitni problemi uočeni kod simetrične kriptografije i to:

- distribucija tajnog ključa (*eng. Key Distribution Problem*). Za šifrovanje podataka koristi se javni ključ, a dešifrovanje podataka može se realizovati samo odgovarajućim privatnim ključem. Stoga se distribucija javnog ključa može obavljati bez značajnih bezbjedonosnih mjera, jer nema opasnosti da se dolaskom u posjed javnog ključa može doći i do povjerljivih podataka;
- za komunikaciju više osoba na bezbjedan način, potrebno je da svaka osoba obezbjedi svoj javni i privatni ključ. U situaciji gdje imamo n osoba, pri čemu svaka treba da komunicira sa svim ostalim osobama na bezbjedan način, ukupan broj ključeva koje je potrebno obezbjediti je:

$$\text{Ukupan broj ključeva} = 2n$$

  U ranijem primjeru od 1000 osoba, ukupan broj ključeva je 2000. Ovo je zaista mali broj u poređenju sa simetričnom kriptografijom i upravljanje ovako malim brojem ključeva je jednostavan zadatak. Porast broja ključeva sa porastom broja osoba u sistemu je linearan, stoga je upotreba asimetrične kriptografije za bezbjednu komunikaciju velikog broja ljudi veoma realna;
- s obzirom na to da su javni i privatni ključ povezani i da je moguće dešifrovati poruku privatnim ključem samo ukoliko je ona šifrovana odgovarajućim javnim ključem, moguće je tačno utvrditi koja strana u komunikaciji je kreirala šifrovanu poruku. Ovo je važna osobina koja je dovela do razvoja digitalnog potpisa i pouzdane autentifikacije osoba.

Na žalost, i asimetrična kriptografija ima određene nedostatke, a to su:

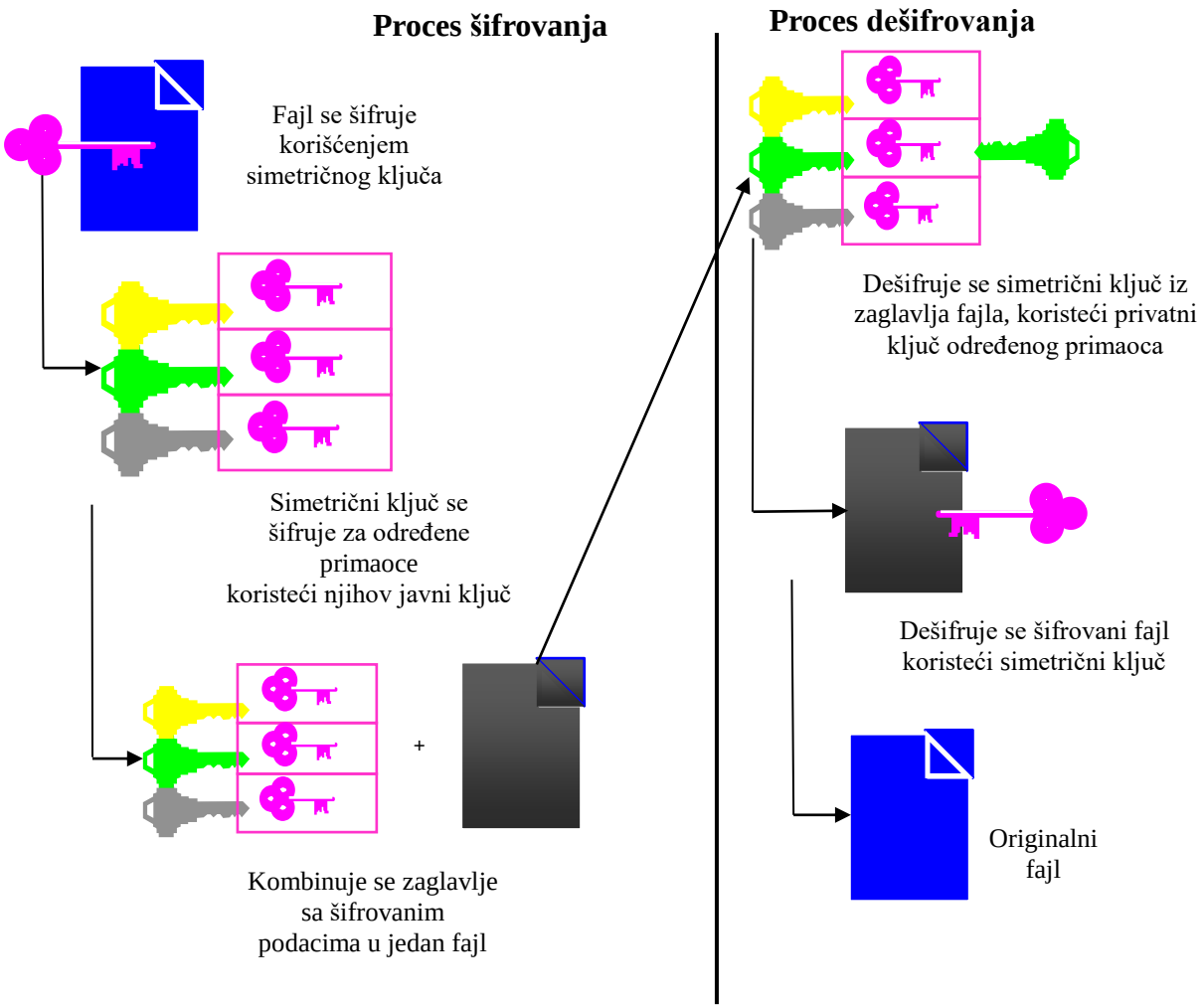
- da bi se šifrovala poruka za osobu A, neophodno je obezbjediti javni ključ osobe A;
- proces šifrovanja podataka, s obzirom na kompleksnost RSA algoritma, je spor i upotreba asimetrične kriptografije je praktična samo za male količine podataka.

2.3 Praktična implementacija – kombinacija simetrične i asimetrične kriptografije

U ranijim poglavljima upoznali smo se sa simetričnom i asimetričnom kriptografijom, kao i dobrim i lošim osobinama svake od njih. Loše osobine onemogućavaju upotrebu

pojedinačnih metoda za šifrovanje velike količine povjerljivih podataka i potrebno je pronaći način kako da se ovi problemi prevaziđu.

Na slici 5 je prikazano korišćenje simetrične i asimetrične kriptografije u procesu kreiranja praktičnog sistema.



***Slika 5**: Šematski prikaz procesa šifrovanja korišćenjem kombinacije simetrične i asimetrične kriptografije*

Opis procesa šifrovanja podataka kod kombinacije simetrične i asimetrične kriptografije:

1. Povjerljivi podaci se šifruju sa simetričnim ključem, koristeći neki od algoritama simetrične kriptografije. S obzirom na to da se koriste algoritmi simetrične kriptografije, vrijeme potrebno za šifrovanje podataka je kratko i moguće je šifrovati velike količine podataka. Simetrični ključ se generiše na slučajan način,

jer se on koristi samo jednom i njegova distribucija se ne obavlja metodama simetrične kriptografije.

2. Simetrični ključ kojim su podaci šifrovani se šifruje javnim ključem primaoca povjerljivih podataka, koristeći neki od algoritama asimetrične kriptografije. Ovaj postupak je moguće ponoviti za više primalaca, šifrujući simetrični ključ odgovarajućim javnim ključem svakog primaoca pojedinačno. S obzirom na to da simetrični ključ sadrži malu količinu podataka, proces njegovog šifrovanja javnim ključevima primalaca je brz, bez obzira na problem performansi asimetrične kriptografije. Podaci dobijeni šifrovanjem simetričnog ključa javnim ključevima primalaca, respektivno, čini zaglavlje (*eng. header*) poruke.
3. Zaglavlje i šifrovani fajl se kombinuju u jedan fajl i šalju na adrese primalaca.
4. Primalac koji ima odgovarajući privatni ključ može da dešifruje zaglavlje poruke koristeći odgovarajući algoritam asimetrične kriptografije i iz njega dobije simetrični ključ kojim je poruka šifrovana.
5. Koristeći simetrični ključ, dešifruje se šifrovani fajl koristeći odgovarajući algoritam simetrične kriptografije i dobije originalni fajl.

Na osnovu svega navedenog, kombinacijom dvije kriptografske metode, dobija se jednostavan i praktičan sistem, kod kojeg su otklonjeni svi nedostaci pojedinačnih metoda, ali i uvedeno značajno poboljšanje mogućnosti slanja povjerljivih podataka na više različitih adresa, bez multiplikacije procesa šifrovanja velike količine podataka.

3 Kvantni kompjuteri

Civilizacija je napredovala kako su ljudi otkrivali nove načine za iskorišćavanje fizičkih resursa, kao što su materijali, sile i energija. U dvadesetom vijeku informacije su dodate ovom spisku, kada je otkriće kompjutera omogućilo kompleksnu obradu informacija koja prevazilazi mogućnosti ljudskog mozga. Istorija razvoja kompjuterskih tehnologija je napredovala u fazama od jednog tipa fizičke realizacije, do drugog tipa: od zupčanika do releja, od releja do ventila, od ventila do tranzistora, od tranzistora do integrisanih kola i tako dalje. Današnje napredne litografske tehnike omogućavaju smještanje logičkih kola širine nekoliko nanometara i žica na površini silikonskih čipova. Uskoro će sa ovim tehnologijama biti moguće kreirati logička kola čak i na manjim površinama i, na taj način, nepovratno dostići tačku gdje će logička kola biti toliko mala da će ih činiti samo nekoliko grupa atoma. Daljim povećavanjem gustine i smanjivanjem veličine logičkih kola, dolazi se do atomskih razmjera gdje materija poštuje pravila kvantne mehanike, koja su različita od pravila klasične fizike koja određuju osobine konvencionalnih logičkih kola. Stoga, ako se nastavi trend razvoja kompjuterske tehnologije i dalje smanjenje veličine logičkih kola, nova kvantna tehnologija mora zamjeniti ili dopuniti tehnologiju koju trenutno poznajemo. Osnovna poenta ovakvog razvoja je da kvantna tehnologija može ponuditi mnogo više od jednostavnog povećavanja gustine logičkih kola i brzine rada mikroprocesora, tj. unapređenja klasičnih kompjutera. Kvantna tehnologija može da podrži potpuno novi način obrade podataka značajno unapređenim algoritmima, baziranim na principima kvantne mehanike. Kompjuteri bazirani na kvantnoj tehnologiji nazivaju se *kvantni kompjuteri*.

3.1 Qubit

Da bi shvatili šta kvantne kompjutere čini toliko različitim u odnosu na klasične kompjutere, potrebno je da napravimo analizu načina čuvanja i obrade informacija, i to počevši od jednog bita – osnovne jedinice za količinu informacija. Sa fizičkog aspekta, bit je fizički sistem koji može biti pripremljen u jednom od dva moguća stanja koji predstavljaju logičke vrijednosti – NE ili DA, NETAČNO ili TAČNO, ili jednostavno 0 ili 1. Na primjer, napon između ploča na kondenzatoru predstavlja jedinicu informacija bit: napunjeni kondenzator označava vrijednost 1, a ispražnjeni kondenzator predstavlja vrijednost 0. Jedan bit informacija može, takođe, biti predstavljen namagnetisanjem dijelova hard diska, dva

različita načina polarizacije svijetlosti, ili dva različita elektronska stanja jednog atoma. Jedan dokument koji se sastoji od n karaktera, a čuva se na hard disku klasičnog kompjutera, predstavljen je sa $(8n)$ nula i jedinica. Ovdje leži jedna od osnovna razlika između klasičnih i kvantnih kompjutera.

Kod kvantnih kompjutera, osnovna jedinica za količinu kvantnih informacija naziva se kvantni bit ili qubit i nije binarna po prirodi. *Qubit* može da postoji u stanjima koja su logička stanja za 0 ili 1 kao kod klasičnog bita, ali i u stanjima koja čine mješavinu ili superpoziciju ovih stanja. Kada govorimo o qubitu u fizičkom stanju koje predstavlja logičku bit vrijednost 0, to stanje qubita označavamo sa $|0\rangle$. Na sličan način, qubit u fizičkom stanju koje predstavlja logičku bit vrijednost 1, označavamo sa $|1\rangle$. Ovo su dva osnovna stanja qubita koja su označena koristeći Dirakove zagrade, da bi se jasno razlikovali od označavanja za klasične bite. Qubit koji se nalazi u fizičkom stanju koje predstavlja superpoziciju, ili linearnu kombinaciju osnovnih stanja, označavamo sa:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

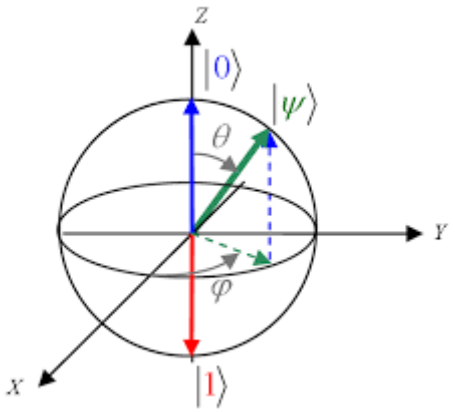
gdje su α i β kompleksni brojevi takvi da vrijedi $|\alpha|^2 + |\beta|^2 = 1$.

Koeficjent α se naziva aplituda komponente $|0\rangle$, a koeficjent β se naziva amplituda komponente $|1\rangle$. Osobina $|\alpha|^2 + |\beta|^2 = 1$ obezbjeđuje da je qubit na pravilan način normalizovan. Pravilna normalizacija qubita garantuje da će qubit tokom finalnog mjerenja njegove bit vrijednosti biti, u stanju $|0\rangle$ sa vjerovatnoćom $|\alpha|^2$ ili u stanju $|1\rangle$ sa vjerovatnoćom $|\beta|^2$, i ne može biti niti u jednom drugom stanju. Na ovaj način zbir vjerovatnoća svih mogućih stanja tokom mjerenja jednak je 1.

S obzirom, da su α i β kompleksni brojevi, mogu se predstaviti na sljedeći način: $\alpha = \cos\left(\frac{\theta}{2}\right)$ i $\beta = e^{i\varphi} sin\left(\frac{\theta}{2}\right)$, gdje je i imaginarna jedinica koja je definisana kao vrijednosti $\sqrt{-1}$. Stoga se qubit u stanju superpozicije može prikazati na sljedeći način:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

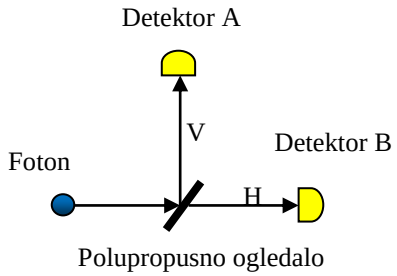
Na osnovu ove formule qubit se može jedinstveno povezati sa tačkom na Bloch sferi, čiji je radijus jednak 1, $0 \leq \theta \leq \pi$ i $0 \leq \varphi \leq 2\pi$, što je prikazano za slici 6.



Slika 6: *Prikaz qubita na Bloch sferi*

S obzirom da svaka od tačaka na Bloch sferi, kojih ima beskonačno mnogo, može da bude bit vrijednost qubita u stanju superpozicije, ovo znači da jedan qubit može da čuva beskonačnu količinu kvantnih informacija. Na žalost mi do svih ovih informacija ne možemo da dođemo jer u procesu mjerenja bit vrijednosti qubita, on zauzima jednu od osnovnih vrijednosti $|0\rangle$ ili $|1\rangle$ sa vjerovatnoćom $|\alpha|^2$ tj. $|\beta|^2$ respektivno. Mjerenje qubita može da bude realizovano u odnosu na bilo koju osu ali osa z je osnovna osa, i ako se mjerenje vrši u odnosu na z osu, ona se naziva računska baza.

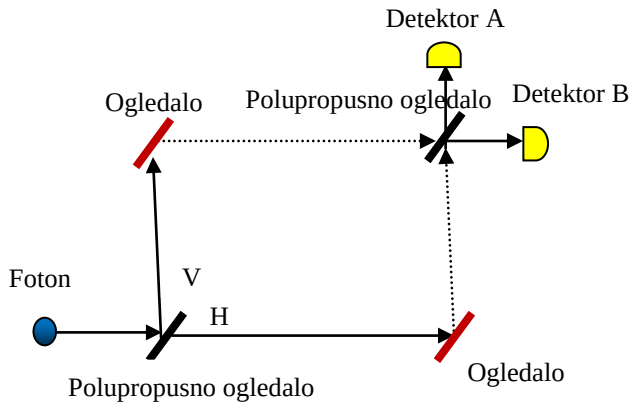
Da bismo približili ideju da jedan kvantni objekat može da bude u više stanja istovremeno, razmotrimo sljedeće eksperimente:



Slika 7: *Interferencija jedne kvantne čestice*

U eksperimentu prikazanom na slici 7, jedan foton se ispali prema polupropusnom ogledalu i detektuje u tački A ili tački B jednakom vjerovatnoćom. Prvo objašnjenje ovakvog ponašanja koje bi nam moglo pasti na pamet je da se foton ne dijeli, nego slučajno (jednakom

vjerovatnoćom) izabere putanju vertikalno, prema tački A, ili horizontalno, prema tački B. Međutim, kvantna mehanika predviđa mogućnost da foton istovremeno putuje u oba pravca i da se pojavljuje u tački A ili tački B, tek nakon realizovanog mjerenja u nekoj od tačaka. Ovaj efekat je poznat kao *interferencija jedne kvantne čestice*.



Slika 8: *Kvantna interferencija*

Na slici 8 je prikazan interesantan eksperiment koji demonstrira efekat kvantne interferencije jedne kvantne čestice. U ovom eksperimentu foton je uvijek detektovan u tački A i nikada u tački B. Ako bi jedan foton nakon prvog polupropusnog ogledala nastavio svoj put vertikalno i reflektovao se od klasičnog ogledala, prema analogiji sa prethodnim eksperimentom, on bi se, jednakom vjerovatnoćom, detektovao i u tački A i u tački B. Isto bi bilo i ako bi foton nastavio svoj put horizontalno. Međutim, rezultati eksperimenta su drastično drugačiji od ovih logičnih zaključaka! Jedino prihvatljivo objašnjenje je da foton istovremeno putuje u oba pravca i da se na raskrsnici formira interferencija takva da je vjerovatnoća da se foton pojavi u tački B jednaka 0. Ovaj efekat je poznat pod imenom *kvantna interferencija* i rezultat je superpozicije mogućih stanja jednog fotona, ili potencijalnih putanja u predmetnom eksperimentu. Iako je samo jedan foton emitovan, iz eksperimenta se nameće mogućnost da identičan foton postoji i putuje suprotnom putanjom od originalnog fotona i on može biti detektovan samo na osnovu efekta interferencije koji se ostvari kada se identični foton sretne sa originalnim fotonom. Ako se, na primjer, bilo koja od putanja blokira potpuno absorbujućim ogledalom, detektor u tački B će početi da registruje fotone baš kao i u prethodnom eksperimentu, tj. jednakom vjerovatnoćom kao i u tački A.

Ova jedinstvena osobina superpozicije mogućih bit stanja kod qubita, pored ostalih osobina kvantne mehanike, omogućava potpuno novi način razmišljanja i kreiranje uređaja sa nevjerovatnim računskim mogućnostima.

3.2 Kvantni memorijski registar

Bilo koji klasični memorijski registar se sastoji od više bita. Klasični kompjuter u bilo kom momentu može da adresira jedan ili više ovih bita. U memorijskom registru, u pojedinim bitima, čuvaju se informacije i nad njima se vrše razne računske operacije. Klasični memorijski registar koji se sastoji od tri bita, može, u jednom momentu, da čuva samo jednu vrijednost od osam mogućih vrijednosti, tj. u jednom momentu, memorijski registar može da bude konfigurisan samo na jedan način od osam mogućih načina 000, 001, 010 … 111.

Slično klasičnom memorijskom registru, neophodno je kreirati i kvantni memorijski registar, koji se sastoji od više qubita. Generalno govoreći, ovo znači da se kvantni memorijski registar sastoji od n qubita, i da je moguće u bilo kom momentu adresirati jedan ili više qubita u kvantnom memorijskom registru, u skladu sa potrebama. Baš kao što jedan qubit može da bude u stanju superpozicije svih mogućih bit vrijednosti, npr. $|0\rangle$ i $|1\rangle$, jedan kvantni memorijski registar koji se sastoji od n qubita može da bude u stanju superpozicije svih mogućih 2^n bit vrijednosti $|00\ldots0\rangle$, $|00\ldots1\rangle$, ..., $|11\ldots1\rangle$. U Kvantni memorijski registar može da se smjesti ista količina različitih brojeva kao i kod klasičnog memorijskog registra. Međutim, u stanju superpozicije, u kvanti memorijski registar u jednom momentu mogu da se smjeste svi mogući brojevi, dok u klasični memorijski registar, u jednom momentu može da se smjesti samo jedan od mogućih brojeva. Kvanti memorijski registar koji se sastoji od tri qubita, u stanju superpozicije, može u jednom momentu da čuva svih osam mogućih brojeva. Ako kvantni memorijski registar proširimo dodatnim qubitima, povećaćemo njegov kapacitet, ali eksponencijalno. Ovo znači da kvantni memorijski registar od četiri qubita može istovremeno da čuva $2^4 = 16$ različitih brojeva… Generalno, kvantni registar sa n qubita može da čuva 2^n različitih brojeva istovremeno.

Opšti način za prikazivanje stanja kvantnog memorijskog registra koji se sastoji od dva qubita je:

$$|\psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

Gdje je $|c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2 = 1$. Odavde vidimo da kvantni memorijski registar možemo posmatrati kao kvantni uređaj koji u istom momentu sadrži različite nizove bit vrijednosti, pri čemu svaki niz ima svoju amplitudu, tj. vjerovatnoću sa kojom može biti izmjeren.

Po analogiji, stanje kvantnog memorijskog registra koji se sastoji od n qubita, možemo prikazati na sljedeći način:

$$|\psi\rangle = c_0|00\ldots0\rangle + c_1|00\ldots1\rangle + \cdots + c_{2^n-1}|11\ldots1\rangle$$

$$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i|i\rangle$$

gdje je $\sum_{i=0}^{2^n-1}|c_i|^2 = 1$, a $|i\rangle$ predstavlja računske baze čije bit vrijednosti odgovaraju decimalnoj vrijednosti broja i koji je predstavljen u binarnom obliku od n cifara, a u kojima se vrši mjerenje kvantnog memorijskog registra.

Kada se jednom kvantni memorijski registar pripremi u stanju superpozicije, moguće je vršiti različite operacije na svim brojevima koji se nalaze u njemu, istovremeno. Ovo znači da kvantni kompjuter može u jednom računskom koraku da realizuje iste matematičke operacije na 2^n različitih brojeva koji su smješteni u kvantnom memorijskom registru od n qubita. Da bi ostvarili isti rezultat na klasičnom kompjuteru, morali bi istu matematičku operaciju ponoviti 2^n puta na jednom procesoru, ili bi morali koristiti paralelnu obradu na 2^n procesora! Drugim riječima, kvantni kompjuteri omogućavaju enormno unapređenje u korišćenju računskih resursa kao što su vrijeme i memorija.

Na osnovu svega, ovo zvuči kao samo još jedno čisto tehnološko unapređenje. Izgleda da klasični kompjuteri mogu da realizuju iste zadatke kao i kvantni kompjuteri, ali za više vremena, ili koristeći više memorije. Osnovna greška kod ovakvog zaključka je što je porast vremena ili memorije eksponencijalan kod klasičnih kompjutera i što bi veoma brzo dostigli nevjerovatno velike vrijednosti, te stoga, klasični kompjuteri ne mogu da realizuju iste zadatke kao i kvantni kompjuteri u realnom vremenu.

3.3 Aplikacije za kvantne kompjutere

Ideja o računskom uređaju koji bi bio baziran na principima kvantne mehanike prvi put se pojavila početkom 1980-ih, u radovima fizičara i kompjuterskih naučnika: Yuri Manin [29], Paul Benioff [30] i [31], i Richard Feynman [32].

Feynman je bio među prvima koji je realizovao teorijski model 1982. godine [32], kojim je mogao da demonstrira mogućnost kako bi kvantni sistem mogao da bude korišćen za izvršavanje računskih operacija. On je, pored ovog, pojasnio kako bi ovakav uređaj mogao da bude korišćen za simulaciju kvantne fizike. Na ovaj način, fizičari bi bili u mogućnosti da realizuju eksperimente iz kvantne fizike unutar kvantnog mehaničkog kompjutera.

Kasnije, 1985. godine, David Deutsch [33] je otkrio da Feymen-ov rad može da se iskoristi za realizaciju kvantnog kompjutera opšte namjene i objavio je ključni teorijski rad u kome je pokazao da bilo koji fizički proces može savršeno da se moduluje sa kvantnim kompjuterom. Nakon ovog rada, a imajući u vidu računsku superiornost kvantnih kompjutera, započela je potraga za aplikacijama koje bi bile adekvatne da se izvršavaju na njima. Prva takva aplikacija se pojavila sa radom Petera Shora 1994. godine [16] u kome je on prezentovao način da se realizuje brza faktorizacija velikih prirodnih brojeva upotrebom kvantnih kompjutera.

Trenutno se radi na pronalaženju dodatnih aplikacija kod kojih bi upotreba kvantnih kompjutera dala značajne rezultate. Treba imati u vidu da je način rada kvantnih kompjutera specifičan, i da oni najvjerovatnije neće biti upotrebljivi u svim aplikacijama. Oblasti u kojima će kvantni kompjuteri dati najveći doprinos su:

- medicina i medicinski materijali. Razumjevanje kompleksnih molekuralnih i hemijskih reakcija dovešće do proizvodnje novih lijekova i medicinskih sredstava;
- distribucija roba. Optimizacije troškova i vremena neophodnih za distribuciju roba dovešće do značajnih promjena u ovoj oblasti;
- vještačka inteligencija. Unapređenje tehnologija vještačke inteligencije, dovešće do značajnog poboljšanja procesa učenja kod mašina, a samim tim i poboljšati tehnike pretraživanja velikih količina podataka, ili mogućnost prepoznavanja slika;
- finansijske usluge i kriptografija. Poboljšanje tehnologija zaštite podataka dovešće do dodatne ekspanzije raznih eServisa.

4 Faktorizacija prirodnih brojeva

Kriptografski sistemi koji se najčešće koriste u svijetu su sistemi asimetrične kriptografije. Bezbjednost najčešće korišćenih algoritama kod asimetrične kriptografije je direktno povezana sa matematičkim problemom faktorizacije prirodnih brojeva. Da bi razumjeli bezbjednost algoritama asimetrične kriptografije i bili u mogućnosti da na deterministički način radimo njenu analizu, neophodno je da se upoznamo sa faktorizacijom prirodnih brojeva.

Prosti brojevi su osnovni blokovi iz kojih možemo, koristeći operaciju množenja, dobiti bilo koji prirodan broj. Postupak zapisa nekog broja u obliku proizvoda odgovarajućih prostih brojeva zovemo faktorizacija. Problem faktorizacije je aktuelan od najranijih vremena. Osim što se radi o važnom problemu u teoriji brojeva, takođe se radi o zahtjevnom problemu iz pozicije složenosti algoritama. Uprkos tome što postoje algoritmi koji brzo, tj. u polinomnom vremenu mogu provjeriti da li je neki broj prost kao što je AKS test prostosti (Agrawal–Kayal–Saxen test prostosti) [27], problem netrivijalne faktorizacije prirodnih brojeva je NP (*eng. Non Polynomial*) problem, tj. trenutno nisu poznati algoritmi koji mogu u polinomnom vremenu netrivijalno faktorizovati velike cijele brojeve sa postojećom tehnologijom na jednom klasičnom kompjuteru ili više njih. Najteže je faktorizovati velike cijele brojeve koji imaju velike proste faktore.

U daljem teksu navodimo neke definicije i teoreme, a vezane za problem faktorizacije brojeva. Ovi pojmovi su sastavni dio svakog predavanja iz teorije brojeva, a na pregledan način su navedeni u [28].

Definicija 1. Faktorizacija matematičkog objekta A je postupak pronalaženja matematičkih objekata A_1,A_2,...,A_n i operacija množenja gdje je $n \in \boldsymbol{N}$ ($\boldsymbol{N}$ je skup prirodnih brojeva), takvih da vrijedi

$$A = A_1 A_2 A_3 \ldots A_n.$$

Kažemo da je A proizvod faktora A_1,A_2,...,A_n.

Napomena 1. U ovom radu ćemo pretpostaviti da vrijedi $0 \notin \boldsymbol{N}$, a sa $\boldsymbol{N_0}$ ćemo označavati skup $\boldsymbol{N} \cup \{0\}$.

Napomena 2. Primijetimo, za $n = 1$ i $A_1 = A$ imamo trivijalnu faktorizaciju $A = A$.

Definicija 2. Neka su a i b cijeli brojevi. Kažemo da a dijeli b (u oznaci $a|b$) ako postoji $k \in \boldsymbol{Z}$ ($\boldsymbol{Z}$ je skup cjelih brojeva) takav da je $b = ak$. Broj a zovemo djelitelj broja b, a broj b djeljenikom broja a. U suprotnom, kažemo da a ne dijeli b i to označavamo sa $a \nmid b$.

Teorema 1. (Teorema o dijeljenju sa ostatkom). Za proizvoljan prirodan broj a i cijeli broj $b \neq 0$ postoje jedinstveni cijeli brojevi q i r, takvi da je $a = qb + r$, $0 \leq r < |b|$.

Broj r zovemo ostatak pri dijeljenju broja a brojem b i to možemo zapisati na sljedeći način: $r = a \bmod b$. U slučaju da je $r = 0$, vrijedi $b|a$.

Definicija 3. Neka su a i b cijeli brojevi. Cijeli broj v nazivamo zajednički sadržalac od a i b, ako $a|v$ i $b|v$. Najmanji nenegativni među njima nazivamo najmanji zajednički sadržalac *od a i b, u oznaci* $\mathrm{NZS}(a, b)$.

Definicija 4. Neka su a i b cijeli brojevi. Cijeli broj d nazivamo zajednički djelitelj od a i b, ako $d|a$ i $d|b$. Ako je barem jedan od brojeva a i b različit od nule, onda postoji samo konačno mnogo zajedničkih djeliteljaa od a i b. Najveći medu njima nazivamo najveći zajednički djelitelj od a i b (ili mjera od a i b), u oznaci (a, b) ili $\mathrm{M}(a, b)$ ili $\mathrm{NZD}(a, b)$.

Teorema 2. (Bezouva lema). Za cijele brojeve a i b vrijedi $(a, b) = \min(\{ax + by \mid x, y \in \boldsymbol{Z}\} \cap \boldsymbol{N})$.

Tvrdnja 1. Ako $d|a$ i $d|b$, onda $d|(ax + by)$ za sve $x, y \in \boldsymbol{Z}$.

Budući da se ostatak dijeljenja dva broja može prikazati kao njihova linearna kombinacija, slijedi posljedica 1.

Posljedica 1. Za sve $n, m \in \boldsymbol{N}$, vrijedi $(n, m) = (m, n \bmod m)$.

Definicija 6. Za cijele brojeve a i b kažemo da su relativno prosti, ako vrijedi $(a, b) = 1$.

Definicija 7. Prirodan broj $p > 1$ je prost, ako za svaki $d \in \{2, 3, \ldots, p - 1\}$ vrijedi $d \nmid p$. Ako prirodan broj $p > 1$ nije prost, onda kažemo da je složen. Broj 1 nije ni prost, ni složen.

Tvrdnja 2. (Euklidova lema). Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Uopštenije, ako $p|a_1a_2 \ldots a_n$, onda p dijeli barem jedan faktor a_i. Dokaze prethodnih teorema i tvrdnji možete naći u [19].

Teorema 3. (Osnovna teorema aritmetike). Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Dokaz. Postojanje faktorizacije dokazujemo indukcijom. Broj 2 je prost i ima trivijalnu faktorizaciju. Pretpostavimo da postoji faktorizacija na proste faktore za sve brojeve manje od n. Ako je n prost broj, on ima primitivnu faktorizaciju. Ako je n složen, tada postoje $1 < n_1, n_2 < n$, takvi da vrijedi $n = n_1.n_2$. Po pretpostavci indukcije postoje prosti brojevi $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$, takvi da vrijedi

$$n_1 = p_1.p_2 \ldots p_k$$

$$n_2 = q_1.q_2 \ldots q_l$$

Tada postoji i faktorizacija na proste faktore broja n

$$n = n_1.\ n_2 = p_1.p_2 \ldots p_k.q_1.q_2 \ldots q_l$$

Sada ćemo dokazati da je faktorizacija broja na proste faktore jedinstvena u odnosu na redosljed faktora. Pretpostavimo da n ima dvije različite faktorizacije na proste faktore, takve da se jedna faktorizacija ne može dobiti iz druge zamjenom poretka faktora. Dijelimo te reprezentacije sa prostim brojevima koji su zajednički obijema reprezentacijama. Budući da su reprezentacije različite, dobićemo jednakost oblika

$$p_1.p_2 \ldots p_r = q_1.q_2 \ldots q_s$$

gdje su p_i,q_j prosti brojevi takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani, tj. $p_i \neq q_j$ za sve i, j. Međutim, to je nemoguće, jer iz $p_i | q_1.q_2 \ldots q_s$, po prethodnoj Euklidovoj lemi, slijedi da p_i dijeli barem jedan q_j. Ali, to znači da je $p_i = q_j$, čime smo dobili kontradikciju s činjenicom da se niti jedan prost broj s lijeve strane jednakosti ne pojavljuje na desnoj strani.

Ako sa p_i označimo i-ti prost broj, onda iz osnovne teoreme aritmetike slijedi da za svaki prirodan broj n vrijedi

$$n = p_1^{\alpha_1}.\ p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

gdje su α_1,α_2,...,α_k nenegativni cijeli brojevi, a p_k najveći prost broj koji dijeli n. Ovakav prikaz broja n zovemo kanonski razvoj broja n na proste faktore. Budući da za svaki $l > k$ i α_{k+1}, α_{k+2},..., $\alpha_i = 0$ vrijedi

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{i=1}^{l} p_i^{\alpha_i}$$

kanonski razvoj broja n na proste faktore možemo označiti sa

$$n = \prod_i p_i^{\alpha_i}$$

Neka prirodni brojevi a i b imaju sljedeće kanonske razvoje na proste brojeve

$$a = \prod_i p_i^{\alpha_i}, b = \prod_i p_i^{\beta_i}$$

Iz definicije najmanjeg zajedničkog sadržaoca slijedi da on očito mora imati sljedeći kanonski razvoj na proste brojeve

$$\text{NZS}(a, b) = \prod_i p_i^{\max(\alpha_i, \beta_i)}$$

Analogno, najveći zajednički djelitelj mora imati sljedeći kanonski razvoj na proste brojeve

$$(a, b) = \prod_i p_i^{\min(\alpha_i, \beta_i)}$$

Tvrdnja 3. Neka su a, b, c i d neki cijeli brojevi. Ako vrijedi $a|b$ i $c|d$, onda vrijedi i $ac|bd$.

Dokaz. Pretpostavimo da vrijedi $a|b$ i $c|d$. Tada postoje cijeli brojevi k_1 i k_2 takvi da vrijedi $b = k_1$a i $d = k_2 c$. Množenjem prethodnih jednakosti, dobijamo $bd = (k_1 k_2)ac$.

Tvrdnja 4. Neka su a, b i n neki prirodni brojevi. Ako $a|n$ i $b|n$, onda vrijedi $\text{NZS}(a, b)|n$.

Dokaz. Pretpostavimo da brojevi a, b i n imaju sljedeće kanonske razvoje na proste faktore

$$a = \prod_i p_i^{\alpha_i}, b = \prod_i p_i^{\beta_i}, n = \prod_i p_i^{\eta_i}$$

Iz $a|n$ slijedi da za svaki i vrijedi $\eta_i \geq \alpha_i$, a iz $b|n$ slijedi da za svaki i vrijedi $\eta_i \geq \beta_i$, stoga očito za svaki i vrijedi $\eta_i \geq \max(\alpha_i, \beta_i)$. Zaključujemo da za svaki i vrijedi $p^{\max(\alpha_i, \beta_i)}|p^{\eta_i}$. Konačno, po prethodnoj propoziciji slijedi

$$\text{NZS}(a, b) = \prod_i p^{\max(\alpha_i, \beta_i)} = \prod_i p^{\eta_i} = n$$

Tvrdnja 5. Neka su a, b i n neki prirodni brojevi. Ako $n|ab$, onda vrijedi $n|(a, n)(b, n)$.

Dokaz. Dajemo kanonske razvoje na proste faktore brojeva a, b i n

$$a = \prod_i p_i^{\alpha_i}, b = \prod_i p_i^{\beta_i}, n = \prod_i p_i^{\eta_i}$$

Zbog tranzitivnosti relacije djeljivosti za proizvoljan prirodan broj j vrijedi $p_j^{\eta_j} | ab$, odnosno, $p_j^{\eta_j} | p_j^{\alpha_j} p_j^{\beta_j}$, iz čega zaključujemo $\eta_j \leq \alpha_j + \beta_j$, što dalje povlači $\eta_j \leq \min\{\alpha_j, \eta_j\} + \min\{\beta_j, \eta_j\}$. Dakle vrijedi

$$p_j^{\eta_j} \mid p_j^{\min(\alpha_j, \eta_j)} p_j^{\min(\beta_j, \eta_j)}$$

Budući da, očito, $p_j^{\min(\alpha_j, \eta_j)}$ dijeli (a, n), te $p_j^{\min(\beta_j, \eta_j)}$ dijeli (b, n), koristeći Tvrdnju 3 i tranzitivnost relacije dijeljenja, zaključujemo da vrijedi

$$p_j^{\eta_j} \mid (a, n)(b, n)$$

Kako je n najmanji zajednički sadržalac brojeva $p_j^{\eta_j}$, iz prethodne tvrdnje slijedi $n | (a, n)(b, n)$.

Osnovna teorema aritmetike govori da su prosti brojevi osnovni gradivni blokovi pomoću kojih možemo izgraditi bilo koji prirodni broj njihovim množenjem. Postavlja se logično pitanje: koliko ima tih blokova?

Teorema 4. (Euklidova teorema). Prostih brojeva ima beskonačno mnogo.

Dokaz. Pretpostavimo da ima n prostih brojeva, gdje je $n \in \boldsymbol{N}$. Sa p_i ćemo označavati i-ti prost broj, za $i \in \{1,2,\ldots,n\}$. Sada definišemo prirodan broj m na sljedeći način

$$m = 1 + \prod_{i=1}^{n} p_i$$

Broj m je očito složen, jer vrijedi $m > p_n$, a p_n je najveći prost broj. Budući da je m složen, postoji $k \in \{1,2,\ldots,n\}$ takav da vrijedi $p_k | m$. Očito vrijedi i $p_k | \prod_{i=1}^{n} p_i$, pa po Tvrdnji 1, p_k dijeli i razliku

$$\left(1 + \prod_{i=1}^{n} p_i\right) - \prod_{i=1}^{n} p_i$$

Zaključujemo $p_k | 1$, što je kontradikcija. Dakle, prostih brojeva ima beskonačno mnogo.

Definicija 8. Brojevi oblika $2^p - 1$, gdje je p prost broj, zovu se Mersennovi brojevi.

Neki Mersennovi brojevi su prosti, dok su neki složeni, kao npr: $2^{11} - 1 = 23 \cdot 89$. Smatra se da ima beskonačno mnogo prostih Mersennovih brojeva (Lenstra-Pomerance-Wagsta pretpostavka). Do januara 2016. godine, poznato je 49 prostih Mersennovih brojeva. Šest najvećih poznatih prostih brojeva su Mersennovi brojevi. Najveći poznati prost broj je Mersennov broj $2^{74207281} - 1$.

Teorema 5. (Mertensova teorema). Neka je n neki prirodan broj i S skup prostih brojeva. Tada postoji $c > 0$ takav da vrijedi

$$\sum_{\substack{p \in S \\ p \leq n}} \frac{1}{p} = \ln(\ln(n)) + c + O\left(\frac{1}{\ln(n)}\right)$$

Dokaz teoreme je dosta složen. Dio se može naći u [19, str. 26] i drugim djelima teorije brojeva.

Definicija 9. Elektronski potpis je skup podataka u elektronskom obliku koji su pridruženi, ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika.

Definicija 10. Napredni elektronski potpis je elektronski potpis kojim se pouzdano garantuje identitet potpisnika i integritet elektronskih dokumenata i koji ispunjava uslove utvrđene relevantnim zakonima.

Definicija 11. Certifikat – potvrda u elektronskom obliku koja povezuje podatke za provjeru elektronskog potpisa sa nekim licem i potvrđuje identitet tog lica.

4.1 Euklidov algoritam

Euklidov algoritam je jedan od najstarijih algoritama. Formulisao ga je Euklid iz Aleksandrije u 3. v. p. n. e, a osnovna namjena ovog algoritma je određivanje najvećeg zajedničkog djelioca dva broja.

Sam Euklidov algoritam sastoji se u uzastopnoj primjeni tvrđenja iskazanog u Teoremi 1. Neka su a i b zadati cijeli brojevi, pri čemu je $a > b$. Tada su, na osnovu Teoreme 1, jednoznačno određeni nenegativni cijeli brojevi q_i i r_i, $1 \leq i \leq k + 1$, tako da je

$$a = q_1 b + r_1, 0 < r_1 < b;$$

$$b = q_2 r_1 + r_2, 0 < r_2 < r_1;$$

$$r_1 = q_3 r_2 + r_3, 0 < r_3 < r_2;$$

...

$$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}, 0 < r_{k-1} < r_{k-2};$$

$$r_{k-2} = q_k r_{k-1} + r_k, 0 < r_k < r_{k-1};$$

$$r_{k-1} = q_{k+1} r_k + 0, r_{k+1} = 0;$$

Niz gornjih jednakosti nazivamo Euklidovim algoritmom dužine k za brojeve a i b. Riječ algoritam podrazumijeva konačnu automatsku proceduru za postupno rješavanje nekog problema, opis toka nekog procesa ili izrade nekog predmeta.

Brojevi $r_1, r_2, \ldots, r_{k-1}, r_k$ u Euklidovom algoritmu čine opadajući niz prirodnih brojeva manjih od b, što znači da se gore opisani postupak mora završiti poslije konačnog broja koraka. Koristeći ovu činjenicu i prethodnu teoremu, lako se dokazuje da za svaka dva cijela broja postoji jedinstven Euklidov algoritam.

Sada možemo iskazati teoremu koja daje odgovor na pitanje određivanja najvećeg zajedničkog djelioca dva broja.

Teorema 6. Najveći zajednički djelitelj prirodnih brojeva a i b, $b \neq 0$, je broj $(a, b) = r_k$, gde je r_k posljednji pozitivan ostatak dobijen primenom Euklidovog algoritma na prirodne brojeve a i b.

Dokaz: Da dokažemo teoremu, pokazaćemo da su zadovoljena sljedeća dva tvrđenja:

(a) $r_k | a$ i $r_k | b$;

(b) ako $d | a$ i $d | b$, tada $d | r_k$.

Zaista, iz posljednje jednakosti Euklidovog algoritma, slijedi da $r_k | r_{k-1}$. Na osnovu toga i pretposljednje jednakosti, zaključujemo da $r_k | r_{k-2}$. Nastavljajući ovaj postupak dobijamo da $r_k | r_{k-3}, \ldots, r_k | b$, a, onda, iz prve jednakosti slijedi da $r_k | a$, čime smo dokazali da je uslov (a) zadovoljen.

Da dokažemo da je i uslov (b) zadovoljen, pretpostavimo da je d prirodan broj koji dijeli brojeve a i b. Tada iz prve jednakosti Euklidovog algoritma odmah slijedi da $d | r_1$, iz druge da $d | r_2, \ldots, d | r_{k-1}$ i, konačno, iz pretposljednje jednakosti slijedi da $d | r_k$, čime je teorema dokazana.

Pseudokod za računanje Najvećeg zajedničkog djelioca dva broja:

```
Ulaz: prirodni brojevi a i b
Izlaz: najveći zajednički djelitelj brojeva a i b
Sve dok je b ≠ 0 radi
{
      t = b
      b = a mod t
      a = t
}
vrati a;
```

Kako je vremenska složenost osnovnih aritmetičkih operacija polinomna, Euklidov algoritam je polinomne vremenske složenosti $3\ln(b)$ (dokaz pogledajte u [19]), za razliku od izvornog Euklidovog algoritma koji nije polinomne složenosti, jer je se u njemu do ostatka dijeljenja dolazilo na složeniji način.

Euklidov algoritam se koristi u skoro svim savremenim algoritmima za faktorizaciju i zbog toga je naveden u ovom radu, mada, sam po sebi, nije algoritam za faktorizaciju brojeva.

4.2 Eratostenovo sito polja brojeva

Ukoliko nas ne zanima faktorizacija prirodnog broja, već samo odgovor na pitanje je li broj prost ili nije, umjesto faktorizacijskih algoritama koristimo testove prostosti, tj. algoritme koji odlučuju je li zadati broj prost. Svaki faktorizacijski algoritam je ujedno i test prostosti, dok suprotno ne važi. Budući da testovi prostosti ne treba da pronađu sve faktore zadatog broja, oni su vremenski efikasniji od faktorizacijskih algoritama.

U 3 v. p. n. e, grčki matematičar Eratosten osmislio je algoritam Eratostenovo sito polja brojeva i to je prvi poznati test prostosti. Algoritam pronalazi sve proste brojeve manje ili jednake zadatom broju.

Postupak dobijanja prostih brojeva pomoću Eratostenovog sita polja brojeva:

- napišite sve brojeve od 2 do n;
- počevši od prvog broja na spisku (broj dva) precrtajte sa spiska sve brojeve djeljive sa dva i upišite da je dva prost broj;

- ponavljajte postupak sa sljedećim neprecrtanim brojem m. Dakle, precrtajte sve brojeve djeljive sa m, a njega samog obilježite da je prost;
- čim nađemo prost broj m takav da je $m^2 > n$, nemamo potrebu za daljim precrtavanjem. Svi brojevi koji su ostali neprecrtani su prosti brojevi.

Algoritam redom „precrtava" sve brojeve djeljive sa prostim („neprecrtanim") brojevima manjim od $\sqrt{n}$. Za neki prost broj $p < \sqrt{n}$, postoji najviše $\frac{n}{p}$ brojeva koji su djeljivi sa njim, a koji su manji od n, pa će algoritam ukupno precrtati:

$$\sum_{p_i \leq \sqrt{n}} \frac{n}{p_i} = n \sum_{p_i \leq \sqrt{n}} \frac{1}{p_i}$$

brojeva, gdje su p_i prosti brojevi.

Na osnovu **Teoreme 5.** *(Mertensova teorema)* ukupan broj precrtanih brojeva je:

$$n\left[\ln\left(\ln\left(\sqrt{n}\right)\right) + c + O\left(\frac{1}{\ln(\sqrt{n})}\right)\right] \approx n \ln\left(\ln\left(\sqrt{n}\right)\right) = n \ln\left(\frac{1}{2}\ln(n)\right) = n \ln\frac{1}{2} + n\ln\left(\ln(n)\right) \approx n\ln\left(\ln(n)\right)$$

Ako pretpostavimo da je za precrtavanje jednog broja potreban broj operacija $\ln(n)$ tada je složenost Eratostenovog sita polja brojeva: $\mathrm{O}\left(n\ln(n)\ln\left(\ln(n)\right)\right)$

Postoje mnogo efiksaniji algoritmi za određivanje da li je neki broj prost od Eratostenovog sita polja brojeva, ali je ovaj algoritam naveden kao veoma dobar primjer kako se određuje složenost nekog algoritma. Kod skoro svih algoritama koji se bave faktorizacijom brojeva kod određivanja složenosti koriste se navedene Teoreme iz teorije brojeva, pa se na sličan način dobijaju i rezultati koji određuju složenost algoritma, a samim tim i procjene vremena za izvršavanje istog.

4.3 Opšte sito polja brojeva

Trenutno asimptotski najbrži poznati klasični algoritam za faktorizaciju prirodnih brojeva većih od 10^{100} je opšte sito polja brojeva (*eng. General Field Number Sieve – GFNS*), čije vrijeme izvršavanja za prirodni broj n se procjenjuje na:

$$O\left(e^{(1.9\cdot(\ln(n))^{\frac{1}{3}}\cdot(\ln\ln(n))^{\frac{2}{3}})}\right)$$

Algoritam opšteg sita polja brojeva je dosta složen i nije napravljeno njegovo pojašnjenje u ovom radu. Za potrebe analize u ovom radu, dovoljna je samo informacija o složenosti algoritma i procjenjeni broj operacija za njegovo izvršavanje. Detaljne informacije o ovom algoritmu možete pronaći u [28].

4.4 Shorov algoritam kvantne faktorizacije

Problem netrivijalne faktorizacije. Neka je N neparan kompozitni prirodni broj. Pronaći proste faktore broja N.

Poznato je da se navedeni problem može riješiti na način što se izabere slučajan prirodni broj m koji je relativno prost sa datim brojem N i nađe najmanji prirodni broj p, takav da je zadovoljena jednakost:

$$m^p = 1 \bmod N$$

Baš ovaj pristup rješavanju problema faktorizacije je pomogao Shoru da definiše svoj algoritam za kvantnu faktorizaciju prirodnih brojeva.

Shorov algoritam se sastoji od nekoliko koraka, a samo drugi korak zahtijeva korišćenje kvantnih kompjutera. Preostali koraci mogu da se izvršavaju na klasičnim kompjuterima.

Pseudokod Shorovog algoritma za kvantnu faktorizaciju prirodnih brojeva:

Ulaz: prirodni broj N
Izlaz: netrivijalni prosti faktor od N
Korak 1:
Izabrati slučajan prirodni broj m takav da je $2 \leq m \leq N-1$
Koristeći Euklidov algoritam izračunati $\mathrm{NZD}(m, N)$
Ako je $\mathrm{NZD}(m, N) \neq 1$ *vrati m i završi rad;*
Korak 2:
Koristeći kvatni kompjuter odrediti nepoznati period P funkcije: $f(x) = m^x \bmod N$
Korak 3:
Ako je P neparan broj, preći na izvršavanje Koraka 1

Komentar: Vjerovatnoća da P bude neparan broj je $\left(\frac{1}{2}\right)^k$*, gdje je k broj različitih prostih faktora od N*

Izračunati $(m^{\frac{P}{2}}+1)$

Ako je $\left(m^{\frac{P}{2}}+1\right) = 0 \bmod N$*, preći na izvršavanje koraka 1*

Komentar: Vjerovatnoća da je $m^{\frac{P}{2}}+1 = 0 \bmod N$ *manja je od* $\left(\frac{1}{2}\right)^{k-1}$*, gdje je k broj različitih prostih faktora od N*

Korak 4:

Koristeći Euklidov algoritam izračunati $d = \text{NZD}\,(m^{\frac{P}{2}}-1, N)$

Komentar: Pošto je $m^{\frac{P}{2}}+1 \neq 0 \bmod N$*, na jednostavan način se može dokazati da je d netrivijalni prosti faktor od N*

Vrati d;

Na osnovu Shorovog algoritma, problem faktorizacije prirodnih brojeva je sveden na problem traženja perioda P od date periodične funkcije f: $\boldsymbol{N}\rightarrow \boldsymbol{N}$. Može se pokazati da ovaj problem nije računski jednostavniji od problema faktorizacije na klasičnim kompjuterima, ali jeste na kvantnim kompjuterima. Procijenjeni broj koraka koje je potrebno realizovati da bi se rješio problem faktorizacije prirodnih brojeva koristeći Shorov algoritam je $\mathrm{O}\big((\ln N)^2(\ln\ln N)(\ln\ln\ln N)\big)$, a to je polinomno vrijeme u odnosu na broj cifara $\mathrm{O}(\ln N)$ od broja N.

4.5 Rezultati uporedne analize algoritama za faktorizaciju

Da bi mogli napraviti procjenu uticaja najnovijih tehnologija na faktorizaciju velikih prirodnih brojeva, napravljeni su programi koji računaju broj neophodnih računskih operacija kod sljedećih algoritama: Richard Schroeppel, opšte sito brojeva [28] i Shorov algoritam kvantne faktorizacije [16]. Kao referenca je korišćen Richard Schroeppel algoritam za faktorizaciju koji je bio najbrži poznati algoritam u vrijeme objavljivanja RSA algoritma. Neophodno vrijeme za faktorizaciju je računato pod istom pretpostavkom koju su koristili autori RSA algoritma, tj. da se jedna računska operacija izvrši za vrijeme od mikrosekunde [5].

Imajući u vidu ograničenja savremenih kompjutera u pogledu veličine brojeva sa kojima mogu da vrše računske operacije, da bi izračunali broj operacija za brojeve koji imaju 500 ili više cifara napravljena je optimizacija matematičkih formula, koristeći osobine logaritama. U

svim proračunima korišćene su pretpostavke da je N veliki prirodni broj koji se sastoji od D cifara, tako da se njegova aproksimativna vrijednost može prikazati u obliku $N = 10^D$.

Kvanti računar na kome bi se izvršavao Shorov algoritam kvantne faktorizacije morao bi da posjeduje tri kvantna memorijska registra, i na njemu bi se takođe, jedna računska operacija izvršavala za vrijeme od mikrosekunde. Broj qubita koje mora da posjeduje svaki kvantni memorijski registar, da bi mogao da čuva broj N, je:

$$\begin{aligned}\text{Kvantni memorijski registar broj qubita} &= \log_2 N \\ &= \frac{\log N}{\log 2} \\ &= \frac{\log 10^D}{\log 2} \\ &= \frac{D}{\log 2}.\end{aligned}$$

Broj računskih operacija potrebnih za faktorizaciju prirodnih brojeva, koristeći Richard Schroeppel algoritam je:

$$\mathrm{O}(e^{\sqrt{\ln(N)\cdot\ln\ln(N)}}) \text{ ili } \mathrm{O}(e^{\sqrt{\mathrm{D}\cdot\ln(10)\cdot(\ln D+\ln(10))}})$$

Broj računskih operacija potrebnih za faktorizaciju prirodnih brojeva koristeći trenutno najbrži poznati klasični algoritam opšte sito polja brojeva je:

$$O(e^{(1.9\cdot(\ln N)^{\frac{1}{3}}\cdot(\ln\ln N)^{\frac{2}{3}})}) \text{ ili } \mathrm{O}(e^{(1.9\cdot D^{1/3}\cdot(\ln 10)^{1/3}\cdot(\ln D+\ln\ln(10))^{2/3})})$$

Broj računskih operacija potrebnih za faktorizaciju prirodnih brojeva, koristeći Shorov algoritam kvantne faktorizacije je:

$$O((\ln N)^2(\ln\ln N)(\ln\ln\ln N)) \text{ ili } \mathrm{O}(D^2(\ln(10))^2(\ln D+\ln\ln(10))(\ln(\ln D+\ln\ln(10))))$$

Pseudokodovi za računanje neophodnog broja operacija za faktorizaciju broja:

```
Ulaz: prirodni broj BrojCifara
Izlaz: broj operacija za faktorizaciju broja koristeći Richard Schroeppel algoritam
a=exp(((BrojCifara*ln(10))*(ln(BrojCifara)+ln(ln(10))))^(1/2))
Vrati a;

Ulaz: prirodni broj BrojCifara
```

```
Izlaz: broj operacija za faktorizaciju broja koristeći opšte sito polja brojeva
a=exp(1.9*(BrojCifara^(1/3))*(ln(10)^(1/3))*(ln(BrojCifara)+ln(ln(10)))^(2/3))
Vrati a;

Ulaz: prirodni broj BrojCifara
Izlaz: broj operacija za faktorizaciju broja koristeći Shorov algoritam kvantne faktorizacije
a=((BrojCifara^2)*(ln(10)^2)*(ln(BrojCifara)+ln(ln(10)))*(ln(ln(BrojCifara)+ln(ln(10)))))
Vrati a;
```

U tabeli 1 dati su rezultati proračuna neophodnog broja operacija i neophodnih vremena za faktorizaciju koristeći analizirane algoritme i ranije navedene pretpostavke.

Br. Cifara broja N	**Richard Schroeppel broj operacija**	**Richard Schroeppel vrijeme**	**opšte sito polja brojeva broj operacija**	**opšte sito polja brojeva vrijeme**	**Shorov algoritam kvantne fakt. broj operacija**	**Shorov algoritam kvantne fakt. vrijeme (u sekundama)**
50	1.4×10^{10}	3.9 sati	2.2×10^{11}	60 sati	97967	9.8×10^{-2}
75	9.0×10^{12}	104 dana	5.1×10^{13}	589 dana	251852	0.25
100	2.3×10^{15}	74 godina	4.4×10^{15}	139 godina	488411	0.49
200	1.2×10^{23}	3.8×10^{9} godina	2.2×10^{21}	7.1×10^{7} godina	2358601	2.36
300	1.5×10^{29}	4.9×10^{15} godina	3.2×10^{25}	1.0×10^{12} godina	5857473	5.86
500	1.3×10^{39}	4.2×10^{25} godina	6.2×10^{31}	2.0×10^{18} godina	18244932	18.24
2000					381450433	381.45

Tabela 1: *Prikaz neophodnih vremena za faktorizaciju broja N koristeći algoritme: Richard-Schroeppel, opšte sito polja brojeva i Shorov algoritam kvantne faktorizacije*

Na osnovu dobijenih rezultata, lako je zaključiti da je napravljeno značajno unapređenje klasičnih algoritama za faktorizaciju, ali da oni i dalje nemaju značajan uticaj na vrijeme faktorizacije velikih brojeva. Sa druge strane, potpuno je drugačija situacija kod upotrebe Shorovog algoritma kvantne faktorizacije, jer je vrijeme potrebno za faktorizaciju izuzetno velikih brojeva jednako stotinama sekundi.

4.6 RSA algoritam i Shorov algoritam kvantne faktorizacije

Diffie, Helman i Merkle su u svom radu iz 1976. godine [4], pored teorijskog koncepta asimetrične kriptografije, patentirali novi sistem za distribuciju simetričnog ključa, ali nisu predložili konkretan algoritam koji bi zadovoljavao definisane zahtjeve asimetrične kriptografije. Konkretan algoritam su predložili Ronald Rivest, Adi Shamir i Leonard Adleman u svom radu iz 1977. godine [5]. Algoritam je dobio naziv po svojim autorima RSA algoritam asimetrične kriptografije.

Osnovni pojmovi kod RSA algoritma:

- parametri p i q, jako veliki prosti brojevi;
- parametar n koji se naziva *modulo.* n je jednako proizvodu parametara p i q*;*
- parametar e koji se naziva *javni eksponent;*
- parametar d koji se naziva *privatni eksponent;*
- javni ključ koji se sastoji iz modulo n i javnog eksponenta e;
- privatni ključ koji se sastoji iz modulo n i privatnog eksponenta d.

Privatni i javni ključ se generišu na sljedeći način:

1. generiše se par jako velikih prostih brojeva p i q;
2. izračuna se modulo n, kao proizvod p i q: $n = pq$;
3. izabere se neparan broj između 3 i n-1 koji je relativno prost u odnosu na brojeve p -1 i q-1, i ovo je javni eksponent e;
4. izračuna se privatni eksponent d na osnovu e, p i q na sljedeći način:
    a. Neka je $L = \text{NZS}(p-1, q-1)$ najmanji zajednički sadržalac brojeva p -1 i q-1;
    b. Bilo koji prirodni broj d koji zadovoljava kongruentnost $de \equiv 1 \bmod L$, je privatni eksponent;

5. objavi se par (n,e) kao javni ključ korisnika, a par (n,d) je privatni ključ korisnika.

Proces šifrovanja kod RSA kriptosistema se realizuje stepenovanjem poruke m sa eksponentom e, po modulu n:

$$c = \text{Encrypt}\,(m) = m^e \bmod n$$

Originalna poruka M se transformiše u nešifrovanu poruku m, na takav način, da je m broj manji od n-1. Ukoliko je poruka M velika ona se podijeli na više poruka, tako da ni jedna nije veća od n-1, i svaka od ovih poruka se šifruje na navedeni način.

Proces dešifrovanja kod RSA kriptosistema se realizuje stepenovanjem šifrovane poruke c sa eksponentom d, po modulu n:

$$m = \text{Decrypt}\,(c) = c^d \bmod n$$

Odnosi između eksponenata e i d garantuju da su šifrovanje i dešifrovanje inverzne transformacije, tako da će se realizovanjem dešifrovanja dobiti originalna poruka m.

Proces elektronskog potpisa kod RSA kriptosistema se realizuje stepenovanjem poruke m sa eksponentom d, po modulu n:

$$s = \text{Sign}\,(m) = m^d \bmod n$$

Proces verifikacije elektronskog potpisa kod RSA kriptosistema se realizuje stepenovanjem elektronski potpisane poruke s sa eksponentom e, po modulu n:

$$m = \text{Verify}\,(s) = s^e \bmod n$$

Jedna od jako korisnih osobina RSA algoritma je činjenica da se isti matematički aparat koristi i za šifrovanje i za dešifrovanje poruka. Razlika je samo u eksponentu sa kojim se stepenuje poruka. Na ovaj način praktična implementacija algoritma se značajno pojednostavljuje.

Bez privatnog ključa (n,d) (ili prostih brojeva p i q), izuzetno je teško dobiti poruku m na osnovu šifrovane poruke c. Na osnovu detaljnih analiza, generalni zaključak je da bilo koja metoda koja se primjeni ne bi bila jednostavnija, ili manje računski zahtijevna od faktorizacije broja n. Stoga je generalno prihvaćeno da je bezbjednost RSA algoritma bazirana na računskoj kompleksnosti faktorizacije velikih brojeva. Faktorizacija velikih prirodnih brojeva, sa pozicije složenosti algoritama, spada u NP algoritam, što znači da na

klasičnom kompjuteru ili više njih, nije moguće faktorizovati veliki prirodni broj u polinomnom vremenu.

Pored računske kompleksnosti problema koja garantuje bezbjednost nekog kriptosistema, generalno prihvaćen stav je da neki kriptografski sistem može da bude proglašen za bezbjedan, tek nakon provjere od strane stručne javnosti i drugih zainteresovanih strana za provjeru. U ovom dijelu, u momentu patentiranja, za RSA algoritam je smatrano da je prošao i ovu provjeru pošto je problem faktorizacije velikih prirodnih brojeva jedan od najstarijih matematičkih problema na čijem rješavanju su radili najpoznatiji naučnici i matematičari u istoriji.

S obzirom na evidentni razvoj tehnologije kvantnih kompjutera, Shorovog algoritma kvantne faktorizacije, rezultata analize uticaja ovih tehnologija na faktorizaciju velikih brojeva i činjenice da je bezbjednost RSA algoritma asimetrične kriptografije direktno povezana sa problemom faktorizacije velikih brojeva, jasno je da ove tehnologije imaju veliki uticaj na bezbjednost RSA algoritma. Imajući u vidu da je RSA algoritam jedan od osnovnih algoritama asimetričnih kriptografskih sistema, koji se kategorišu kao savremeni kriptografski sistemi, Shorov algoritam kvantne faktorizacije, u ovom momentu, ima veliki uticaj na bezbjednost savremenih kriptografskih sistema.

5 Kvantna kriptografija i period nakon kvantnih kompjutera

U prethodnom dijelu rada napravljen je detaljan pregled klasičnih kriptografskih sistema, novih tehnologija i analiza njihovog uticaja na savremene kriptografske sisteme. Rezultati analize su indikativni i neophodno je započeti potragu za novim kriptografskim tehnologijama koje će eliminisati uticaj uočenih prijetnji, tj. rizike, koje imaju nove tehnologije na bezbjednost savremenih kriptografskih sistema. Postoje dva moguća pravca za otklanjanje rizika i to su: 1. pronalaženje novih algoritama koji su otporni na prijetnje koje donose kvanti kompjuteri, i koji će se upotrebljavati u postojećim kriptografskim sistemima; 2. pronalaženje novih kriptografskih sistema koji su otporni na prijetnje koje donose kvanti kompjuteri , i po mogućnosti su bezuslovno bezbjedni.

U nastavku rada su razmatrane nove kriptografske tehnike koje nude veliki potencijal za eliminaciju rizika koje donose kvantni kompjuteri. Sagledana je mogućnost kombinacije novih kriptografskih tehnika sa već poznatim kriptografskim sistemima, u cilju kreiranja bezuslovno bezbjednog kriptografskog sistema.

5.1 Kvantna kriptografija

Na osnovu razmatranja koja smo napravili, može se uočiti da je osnovni problem klasičnih simetričnih kriptografskih sistema činjenica da se bezbjedna komunikacija može započeti tek nakon što je razmjenjen tajni ključ, koristeći potpuno bezbjedan komunikacioni kanal. Ovakva situacija se u logici uobičajeno naziva *paradoks 22*, i označava situacije iz kojih pojedinac ne može da pobjegne zbog kontradiktornih uslova.

Paradoks 22: Prije nego što `Alice` i `Bob` mogu komunicirati bezbjedno, oni moraju komunicirati bezbjedno.

Pored predmetnog postoji i sljedeći paradoks: *paradoks 22a*.

Paradoks 22a: Čak i ako `Alice` i `Bob`, na neki način, uspiju da razmijene njihov tajni ključ preko bezbjednog komunikacionog kanala, u klasičnoj kriptografiji ne postoji nikakav mehanizam koji će garantovati potpuno sigurno da je njihov tajni ključ razmijenjen bezbjedno, tj. ne postoji način koji će garantovati da je njihov bezbjedan komunikacioni

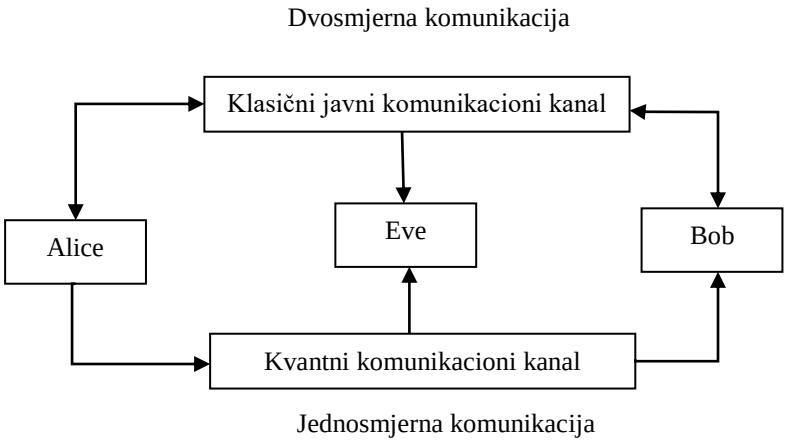
kanal zaista bezbjedan i da ne postoji neovlašćena osoba Eve koja nadgleda njihovu komunikaciju (špijunira).

Trajno rješenje za uočene paradokse je upotreba sistema bezbjednog prenosa podataka zasnovanih na osnovnim principima kvantne mehanike – kvantne kriptografije. Isti fizički principi koji su doveli do razvoja kvantnih kompjutera i narušavanja bezbjednosti asimetrične kriptografije su rješenje predmetnih paradoksa koji onemogućavaju praktičnu upotrebljivost sistema simetrične kriptografije.

Dvije osnovne funkcionalnosti koje obezbjeđuje kvantna kriptografija su:

- omogućava da dvije strane, u našem slučaju Alice i Bob, razmjene slučajni ključ na bezbjedan način. Ova funkcionalnost je poznata pod nazivom kvantna distribucija ključeva;
- omogućava pouzdano detektovanje neovlašćenog prisluškivanja komunikacije ukoliko je prisutno, što klasični sistemi razmjene poruka nikako ne mogu da obezbjede.

Na slici 9 prikazana je šema komunikacionog sistema kvantne kriptografije:



Slika 9: *Komunikacioni sistem kvantne kriptografije za bezbjednu razmjenu slučajnog ključa*

Kod kvantne distribucije ključeva, jedna kvantna čestica pripremljena na odgovarajući način se šalje od Alice do Boba (jednosmerna komunikacija). Alice i Bob komuniciraju preko dva komunikaciona kanala: kvantni komunikacioni kanal, putem koga se šalju kvantne čestice od pošiljaoca do primaoca, i klasični javni komunikacioni kanal preko koga razmjenjuju podatke koji nisu povjerljivi. Ukoliko Eve nadgleda komunikaciju preko

kvantnog komunikacionog kanala, `Alice` i `Bob` će ovo da otkriju u okviru komunikacije koju obavljaju preko klasičnog javnog komunikacionog kanala. Ovo je omogućeno zahvaljujući zakonima kvantne mehanike definisanim kroz Hajzenbergov princip neodređenosti [8], i to:

- Bilo koje mjerenje koje be `Eve` napravila mora da izazove promjene u kvantnom stanju sistema;
- `Eve` ne može da napravi kopiju proizvoljnog kvantnog stanja.

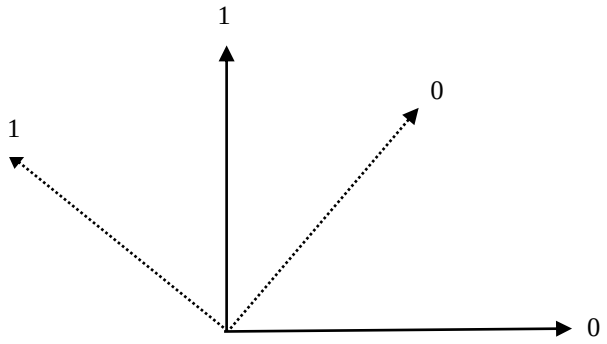
5.1.1 BB84 protokol za kvantnu distribuciju ključeva

Prvi protokol koji je omogućio korišćenje kvantne kriptografije, a koristi se za kvantnu distribuciju ključeva, predložili su Charles Bennett i Gilles Brassard 1984 godine, zbog čega je i dobio naziv „BB84 protokol" [10].

BB84 protokol je zasnovan na korišćenju impulsa polarizovane svjetlosti, pri čemu svaki impuls sadrži samo jedan foton. `Alice` i `Bob` su povezani sa kvantnim komunikacionim kanalom kao što je, npr. optičko vlakno i klasičnim javnim komunikacionim kanalom kao što je, npr. telefonska linija ili internet konekcija. U praksi uobičajeno je da se koristi ista linija za oba komunikaciona kanala. Ukoliko se za prenos informacija koristi polarizovani foton, to može biti optičko vlakno, koje se razlikuje samo po intenzitetu svjetlosnih impulsa: za kvantni komunikacioni kanal za jedan bit informacija šalje se samo jedan foton, a za klasični javni komunikacioni kanal za jedan bit informacija šalje se na stotine fotona.

Kodna šema u okviru BB84 protokola (kvantni alfabet) povezuje jedan bit informacija sa određenim kvantnim stanjima fotona i to, na takav način, da svakom bitu informacija odgovara kombinacija od dva jednako vjerovatna neortogonalna kvantna stanja.

Na slici 10 prikazana su dva neortogonalna stanja fotona kada se koristi polarizacija fotona kao nosilac informacija.



Slika 10: *Prikaz neortogonalnih kvantnih stanja fotona ukoliko se koristi polarizacija fotona*

Sa slike 10 se jasno vidi da se koriste dvije baze i to: pravougaona koju ćemo označavati sa $+$, i dijagonalna koju ćemo označavati sa $\times$. U okviru ove dvije neortogonalne baze foton može imati ukupno 4 različita stanja u smislu polarizacije i njih označavamo na sljedeći način:

$+$ pravougaona baza • Horizontalna polarizacija $\|\leftrightarrow\rangle$ • Vertikalna polarizacija $\|\updownarrow\rangle$	$\times$ dijagonalna baza • $+45^o$ polarizacija $\|\nearrow\rangle$ • -45^o ili $+135^o$ polarizacija $\|\searrow\rangle$

Povezivanje polarizacija fotona sa informacijama nazivamo kvantni alfabet i, u zavisnosti od baza za polarizaciju koje se koriste, imamo dva kvantna alfabeta:

A_+- kvantni alfabet za pravougaonu polarizaciju

Simbol	**Bit**
$\|\leftrightarrow\rangle$	0
$\|\updownarrow\rangle$	1

$A_\times$ - kvantni alfabet za dijagonalnu polarizaciju

Simbol	**Bit**
$\|\nearrow\rangle$	0
$\|\searrow\rangle$	1

Proces kvantne distribucije ključeva putem BB84 protokola odvija se u dva koraka:

Korak I: Komunikacija preko kvantnog kanala

1. `Alice` mora, svaki put kada treba da pošalje jedan bit informacija, da na slučajan način, a sa jednakom vjerovatnoćom, izabere jedan od dva neortoganalna kvantna alfabeta A_+ ili $A_\times$. Koristeći izabrani kvantni alfabet, foton se polarizuje na odgovarajući način i šalje `Bob`u. `Alice` zapamti koji je kvantni alfabet koristila za svaki foton.

   Napomena 1*: Ovdje je korisno skrenuti pažnju da je u praksi teško realizovati sistem koji na slučajan način bira moguća stanja za polarizaciju fotona*

2. `Bob` vrši mjerenje polarizacije dolazećih fotona koristeći jedan od dva moguća kvantna alfabeta A_+ili $A_\times$, ali njihov izbor vrši na slučajan način sa jednakom vjerovatnoćom i sasvim nezavisno od `Alice`. Ako `Alice` i `Bob` koriste isti kvantni alfabet, onda će dobiti savršeno podudarne rezultate, tj. `Bob` će detektovati foton sa identičnom polarizacijom koju je `Alice` koristila kod slanja fotona, a to znači identičan bit koji je `Alice` poslala. Međutim, svaki put kada `Bob` koristi drugi kvantni alfabet u odnosu na onaj koji je koristila `Alice` kod slanja fotona, situacija je drugačija. Na primjer, ako `Alice` pošalje horizontalno polarizovan foton $|\leftrightarrow\rangle$ i Bob mjerenje izvrši koristeći kvanti alfabet $A_\times$, on će sa vjerovatnoćom od 50% dobiti ili $+45^o$ ili -45^o polarizovani foton. Ovo znači da će, u ovom slučaju, `Bob` sa vjerovatnoćom od 50% dobiti identičan bit informacije koji je `Alice` poslala. Čak i ako bi `Bob` ustanovio da je koristio pogrešan alfabet, on nema nikakve mogućnosti da otkrije sa kojom polarizacijom je bio foton koji je `Alice` poslala. U pojedinim situacijama `Bob` neće detektovati nikakav signal zbog nesavršenosti opreme: uređaja za slanje, kvantnog komunikacionog kanala, ili uređaja za prijem.

3. Nakon završenog procesa slanja, `Bob` će imati niz primljenih bita, tzv. sirovi ključ (*eng. raw key*).

   Napomena 2*: Vjerovatnoća da `Bob` primi korektno bit koji je `Alice` poslala, u najboljem slučaju iznosi:*

$$\mathrm{P}_{\text{poslati i primljeni bit su jednaki}} = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$$

$$P_{\text{poslati i primljeni bit su različiti}} = 1 - \frac{3}{4} = \frac{1}{4}$$

Napomena 3: *Za svaki bit informacija koji* `Alice` *pošalje* `Bob`*u, postoje dva moguća scenarija za* `Eve`***:***

- *ona nadgleda prenos bita sa vjerovatnoćom* $0 < \beta < 1$ *(Ako je* $\beta = 1$*, ovo znači da se nadgleda svaki bit prenosa);*
- *ona ne nadgleda prenos bita sa vjerovatnoćom* $1 - \beta$ *(Ako je* $\beta = 0$*, ovo znači da se ne nadgleda niti jedan bit prenosa).*

S obzirom na to da `Bob` *i* `Eve`*, sasvim slučajno i potpuno nezavisno jedno od drugog i potpuno nezavisno od kvantnog alfabeta koji je izabrala* `Alice`*, biraju kvantni alfabet kojim će vršiti mjerenje, nadgledanje prenosa od strane* `Eve` *imaće trenutan i primjetan uticaj na tačnost bita koje prima* `Bob`*. Ovaj uticaj se ogleda u povećanju broja pogrešnih bita koje* `Bob` *prima, sa* $\frac{1}{4}$ *na:*

$$\frac{1}{4} \cdot (1 - \beta) + \frac{3}{4} \cdot \frac{\beta}{2} = \frac{1}{4} + \frac{\beta}{8}$$

Iz ove formule se vidi da će se vjerovatnoća greške sa $\frac{1}{4}$ *povećati na* $\frac{3}{8}$*, u slučaju da* `Eve` *nadgleda svaki bit prenosa, što je povećanje od 50%. Na ovaj način, mjerenjem procenta pogrešnih bita, nepobitno se može utvrditi prisustvo neovlašćene osobe koja nadgleda prenos.*

Korak II: Komunikacija preko klasičnog javnog kanala

Korak II. Faza 1: Izdvajanje tačno primljenih podatka iz sirovog ključa

4. Namjena ovog dijela protokola je da se detektuju pozicije bita i uklone biti sa tih pozicija, na kojima se mogla javiti greška čak i bez nadgledanja komunikacije od strane `Eve`. Da bi se postigao cilj putem klasičnog javnog komunikacionog kanala za svaku poziciju bita `Bob` šalje informacije o kvantnom alfabetu koji je koristio i da li je detektovao signal. Naravno, `Bob` ne otkriva i koju je vrijednost dobio putem mjerenja.
5. Nakon poređenja informacija o kvantnim alfabetima koje je koristio `Bob` i koje je koristila `Alice`, `Alice` putem klasičnog javnog komunikacionog kanala javlja `Bob`u na kojim pozicijama je koristio korektan kvantni alfabet i oni zadržavaju

bite samo na tim pozicijama. Ključ koji se dobije nakon ove dvosmjerne komunikacije naziva se prosijani ključ.

Napomena 4*: Ukoliko nema nadgledanja komunikacije, prosijani ključ koji ima* `Alice` *i prosijani ključ koji ima* `Bob`*, biće identični. Sa druge strane, ukoliko* `Eve` *nadgleda komunikaciju, odgovarajući biti u prosijanim ključevima kod* `Alice` *i* `Bob`*a razlikovaće se sa vjerovatnoćom:*

$$0 \cdot (1 - \beta) + \frac{1}{4} \cdot \beta = \frac{\beta}{4}$$

Korak II. Faza 2: Provjera da li postoji nadgledanje komunikacije, kroz provjeru grešaka u prenosu

6. `Alice` i `Bob` iz prosijanog ključa izaberu dogovoreni broj bita m na slučajnim pozicijama. Kroz dvosmjernu komunikaciju putem klasičnog javnog komunikacionog kanala oni porede svaki bit pojedinačno i računaju broj različitih bita. Biti sa izabranih pozicija se nakon provjere odbacuju, bez obzira da li se razlikuju ili ne. U slučaju da se tokom poređena otkrije razlika čak i u jednom bitu, ovo znači da `Eve` nadgleda komunikaciju, tako da se proces prekida i `Alice` i `Bob` započinju kompletan proces ponovo počevši od koraka 1, tj. od početka. Proces se ponavlja sve dok ne dobiju test u kome nema nikakvih razlika, tako da je jasno da je prosijani ključ skraćen za dodatnih m bita, njihov konačni tajni ključ.

   Napomena 4*: Razlike u testiranim bitima mogu da se jave zbog nadgledanja kanala od strane* `Eve`*, ali i zbog tehničkih nesavršenosti opreme. U slučaju da* `Alice` *i* `Bob` *ne pronađu razliku ni u jednom bitu, vjerovatnoća da je nadgledanje komunikacije od strane* `Eve` *prošlo neotkriveno je:*

$$\mathrm{P}_{\text{neotkriveno}} = \left(1 - \frac{\beta}{4}\right)^{m}$$

   Npr. za $\beta = 1$ i $m = 200$

$$\mathrm{P}_{\text{neotkriveno}} = \left(1 - \frac{1}{4}\right)^{200} \approx 10^{-25}$$

   U slučaju da je predmetna vjerovatnoća dovoljno mala, tj. u skladu sa dogovorenim vrijednostima između `Alice` *i* `Bob`*a, oni mogu da donesu odluku*

da je kanal bez nadgledanja i da zajednički usaglase da je prosijani ključ skraćen za dodatnih m bita, njihov konačni tajni ključ.

Napomena 5*: Dobijeni konačni tajni ključ je slučajan, jer su i* `Alice` *i* `Bob` *na sasvim slučajan način i nezavisno, birali kvantne alfabete kod slanja i prijema signala.*

U tabeli 2 je prikazan opisani proces razmjene ključa koristeći BB84 protokol.

`Alice` bit vrijednosti	1	0	0	1	0	**0**	0	1	1
`Alice` kvantni alfabet	$A_\times$	A_+	A_+	A_+	$A_\times$	$A_\times$	A_+	$A_\times$	A_+
`Alice` polarizacija fotona	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nwarrow\rangle$	$\|\updownarrow\rangle$
`Bob` kvantni alfabet	$A_\times$	$A_\times$	A_+	$A_\times$	A_+	$A_\times$	$A_\times$	A_+	A_+
`Bob` polarizacija fotona	$\|\nwarrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	-	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$
`Bob` bit vrijednost (sirovi ključ)	1	1	0	1	0	0	-	1	1
Isti kvantni alfabet?	Da	Ne	Da	Ne	Ne	Da	Ne	Ne	Da
`Bob` prosijani ključ	1	-	0	-	-	**0**	-	-	1
`Eve` test (provjera nadgledanja?)	Ne	-	Ne	-	-	**Da**	-	-	Ne
Tajni ključ	**1**	**-**	**0**	**-**	**-**	**-**	**-**	**-**	**1**

Tabela 2: *Primjer generisanja tajnog ključa koristeći BB84 protokol*

5.2 Savršena bezbjednost

Prethodno smo u poglavlju Asimetrična kriptografija, naveli da je jedan od osnovih ciljeva kriptografije pronalaženje neprobojnih kriptografskih sistema. Uobičajeno tumačenje neprobojnog kriptografskog sistema je da je to sistem kod koga se ne može napraviti dešifrovanje šifrovane poruke bez poznavanja odgovarajućeg ključa sa kojim je poruka šifrovana. Međutim, ovakvo opšte shvatanje ili formulacija ne omogućavaju pouzdanu analizu i matematički dokaz da je neki sistem stvarno neprobojan. Zbog toga se za određene sisteme nagađa da su neprobojni zbog činjenice da niko nije uspio da dešifruje poruke pod

gore navedenim uslovima, ili što je njihova bezbjednost zasnovana na matematički kompleksnim računskim zadacima i ogromnim količinama računskih operacija. Kao što je ranije napomenuto, ovakav način analize je nepouzdan i mnogo puta u istoriji je demantovano da je određeni kriptografski sistem neprobojan, nakon određenog vremena.

Zbog svega ovog, neophodno je matematički definisati šta neprobojnost određenog kriptografskog sistema podrazumjeva. Ovo je prvi uradio Claud Shannon u svom djelu iz 1949. godine [3]. Sisteme koji ispunjavaju Shannonovu matematičku definiciju neprobojnosti nazivamo savršeno bezbjedni (*eng.Perfect Secrecy*). U svom radu, on je dokazao da je OTP sistem, koji je prvi put opisao Gilbert Vernam u svom dijelu iz 1917 godine [6], savršeno bezbjedan. Gilbert Vernam je uvijek tvrdio da je njegov sistem za šifrovanje podataka neprobojan, ali to nikad nije uspio teorijski da dokaže, tako da je Shannonov dokaz prva matematička potvrda da je ovaj metod neprobajan i jedini algoritam koji je matematički dokazano da je neprobojan, do sada.

Definicija 9. Za kriptografski sistem kojeg čine transformacije generisanja ključeva, šifrovanja poruka i dešifrovanja poruka (*eng. Generate, Encrypt, Decrypt*) nad ukupnim prostorom poruka *M*, ukupnim prostorom ključeva *K* i ukupnim prostorom kriptograma *C*, kažemo da je savršeno bezbjedan ako za sve poruke $m_1, m_2 \in M$ i za sve kriptograme $c \in C$ važi:

$$\mathrm{P}[k \leftarrow \mathrm{Generate}: \mathrm{Encrypt}(k, m_1) = c] = \mathrm{P}[k \leftarrow \mathrm{Generate}: \mathrm{Encrypt}(k, m_2) = c]$$

gdje je sa P označena vjerovatnoća dešavanja određenog događaja, i gdje su obe vjerovatnoće računate za izabrani ključ k iz ukupnog prostora ključeva K i ne zavise od izbora konkretnog algoritima za šifrovanje - Encrypt.

- $k \leftarrow Generate$ je konkretan algoritam koji generiše ključ k (možemo smatrati za sada da se k generiše tako što se na slučajan način izabere jedan od mogućih ključeva k iz ukupnog prostora ključeva *K*);
- *Encrypt* je konkretan algoritam sa kojim se šifruju podaci tj. *Encrypt*: $K \times M \rightarrow C$;
- C označava ukupni prostor kriptograma (definisanog na osnovu *Encrypt*, *K*, i *M*);
- *Decrypt* je konkretan algoritam za dešifrovanje kriptograma tj. *Decrypt*: $K \times C \rightarrow M$.

Pojednostavljeno objašnjenje gornje jednakosti: Vjerovatnoća da se dobije kriptogram c šifrujući poruku m_1 sa ključem k, jednaka je vjerovatnoći da se dobije kriptogram c šifrujući

poruku m_2 sa ključem k. Ključ k se bira sasvim slučajno iz ukupnog skupa mogućih ključeva K.

Moguća tumačenja definicije i zahtijeva koje treba da ispunjavaju savršeno bezbjedni kriptografski sistemi:

- za određeni kriptogram, svaka poruka iz ukupnog skupa poruka ima jednaku vjerovatnoću da bude odgovarajuća kodna poruka (*eng. plain text*). Ovo znači da, na osnovu samog kriptograma, nikako nije moguće odrediti da li je nastao na osnovu kodne poruke m_1 ili kodne poruke m_2;
- kodna poruka je u potpunosti nezavisna od kriptograma;
- ukoliko neovlašćeno lice dođe u posjed kriptograma, ono na osnovu istog ne može dobiti baš nikakve informacije o odgovarajućoj kodnoj poruci.

5.2.1 Vernamov One Time Pad (OTP) kriptografski sistem

Vernam je definisao svoj kriptografski sistem na sljedeći način:

M: $\{0,1\}^l$; K: $\{0,1\}^l$; C: $\{0,1\}^l$, gdje je l dužina poruke.

Ukupan prostor poruka M, ukupan prostor ključeva K i ukupan prostor kriptograma C čine svi mogući skupovi 0 i 1 dužine l.

Proces šifrovanja kod OTP kriptosistema se realizuje na sljedeći način:

$c = \text{Encrypt}(k, m) = m \oplus k$, za $m \in M, k \in K$

gdje „$\oplus$" označava operaciju ekskluzivno-ili (XOR između bita, s obzirom da ukupan prostor M i ukupan prostor K čine 0 i 1).

Proces dešifrovanja kod OTP kriptosistema se realizuje na sljedeći način:

$m = \text{Decrypt}(k, c) = c \oplus k$, za $m \in M, k \in K$.

Da bi mogli raditi analizu OTP kriptosistema, potrebno je da smo familijarni sa osobinama operacije XOR:

- $x \oplus 0 = x$. XOR sa 0 dobija se isti broj. Stoga je 0, identitet za XOR operaciju;
- $x \oplus 1 = \overline{x}$. XOR sa 1 dobija se komplement;
- $x \oplus x = 0$. XOR x sa samim sobom dobija se 0;

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$. XOR je asocijativna operacija;
- $x \oplus y = y \oplus x$. XOR je komutativna operacija.

Sve navedene osobine mogu se provjeriti koristeći osnovnu definiciju operacije XOR i tabele tautologije.

S obzirom na definisani način šifrovanja podataka, dokaz da je dešifrovanje podataka moguće, tj. definisano na korektan način:

$$(c \oplus k) = ((m \oplus k) \oplus k) = m \oplus (k \oplus k) = m \oplus 0 = m$$

Primjer:

OTP šifrovanje:

$m = [0110111]$

$k = [1011010]$

$c = [1101101]$

OTP dešifrovanje

$c = [1101101]$

$k = [1011010]$

$m = [0110111]$

Teorema 7. OTP kriptografski sistem je savršeno bezbjedan, odnosno, zadovoljava zahtjeve koje mora da ispuni jedan savršeno bezbjedan kriptografski sistem.

Dokaz: Uzmimo jednu poruku $m \in M$ i $c \in C$, i neka je $k^* = m \oplus c$. Primjetimo da je:

$$\begin{aligned} \mathrm{P}[k \leftarrow \text{Generate}: \mathrm{Encrypt}(k, m) = c] &= \mathrm{P}[k \leftarrow \text{Generate}: k \oplus m = c] \\ &= \mathrm{P}[k \leftarrow \text{Generate}: k = m \oplus c] \\ &= \mathrm{P}[k \leftarrow \text{Generate}: k = k^*] \\ &= \frac{1}{2^l} \end{aligned}$$

S obzirom na to da gornja jednačina važi za svako $m \in M$, slijedi da je za bilo koje poruke m_1 i $m_2 \in M$ imamo:

$$\mathrm{P}[k \leftarrow \text{Generate}: \mathrm{Encrypt}(k, m_1) = c] = \frac{1}{2^l}$$

$$\mathrm{P}[k \leftarrow \text{Generate}: \mathrm{Encrypt}(k, m_2) = c] = \frac{1}{2^l}$$

Na osnovu čega dobijamo da je:

$$P[k \leftarrow \text{Generate: Encyrpt}(k, m_1) = c] = \text{P}[k \leftarrow \text{Generate: Encrypt}(k, m_2) = c]$$

što je definicija zahtijeva koje mora da ispunjava savršeno bezbjedan kriptografski sistem.

Teorema 8. Da bi neki kriptografski sistem bio savršeno bezbjedan kriptografski sistem, on mora da ima istu veličinu ukupnog prostora ključeva *K* i ukupnog prostora poruka *M*. Ako su ključevi i poruke predstavljeni kao binarni stringovi M=$\{0,1\}^l$i $K = \{0,1\}^n$, predmetni kriptografski sistem je savršeno bezbjedan samo ako je $n = l$, tj. dužina poruka *M* je jednaka dužini ključeva *K*.

Dokaz: Pretpostavimo suprotno, tj. da je$|K| < |M|$. Uzmimo neki kriptogram *c* takav da postoji $m^* \in M$ *i* $k^* \in K$ takvi da je $\text{Encrypt}(k^*, m^*) = c$. Izračunajmo broj poruka *m* koje se mogu dobiti dešifrovanjem kriptograma *c* nekim validnim ključem $k \in K$, tj. neka je $S \in M$ skup poruka $S = \{m \mid \exists k \in K \text{ Encrypt}(k, m) = c\}$. Primjetimo da važi $S = \{m = \text{Decrypt}(k, c)\}\ \exists k \in K$ i da za svako $k \in K$ postoji najviše jedna poruka *m*, takva da je $m = \text{Decrypt}(k, c)$, stoga je veličina seta poruka *S*, u najboljem slučaju, jednaka veličini prostora ključeva *K*. Na osnovu ovog zaključujemo da postoji skup poruka koji nije prazan takav da je $S' = M \backslash S$. Za svaku poruku $m \in S'$ ne postoji ključ $k \in K$ takav da je $c = \text{Encrypt}(k, m)$. Drugim riječima, za svaku poruku $m \in S'$ imamo:

$$\text{P}[k \leftarrow \text{Generate: Encrypt}(k, m) = c] = 0$$

Ali, s obzirom na to da postoji $m^* \in M$ i $k^* \in K$ takvi da je $\text{Encrypt}(k^*, m^*) = c$, onda mora postojati ključ *K*, takav da je

$$\text{P}[K \leftarrow \text{Generate: Encrypt}(K, m^*) = c] \neq 0$$

a ovo je u suprotnosti sa prethodnim zaključkom, čime smo dobili kontradiktornost. Na ovaj način smo dokazali da pretpostavka da je$|K| < |M|$ kod savršeno bezbjednih kriptografskih sistema nije dobra, što znači da, u najgorem slučaju, ukupna veličina prostora ključeva *K* mora biti jednaka ukupnoj veličine prostora poruka *M*, a može biti i veća. S obzirom na to da je potrebno optimizovati sistem, jasno je da je dovoljno da je ukupna veličina prostora ključeva *K* jednaka ukupnoj veličini poruka *M* i da će se, na taj način, zadovoljiti zahtijevi za savršeno bezbjednim kriptografskim sistemom.

Zapažanje 1. Ako je $k = \{0\}^n$, onda je $\text{Encrypt}(k, m) = m \oplus k = m \oplus 0 = m$. Ovo znači da je kriptogram jednak poruci, tj. poruka nije šifrovana!

Ideja Ne koristiti $k = \{0\}^n$ u ukupnom prostoru ključeva *K*.

Ovo nije dobra ideja iz sledećeg razloga:

Ako $k = \{0\}^n$nije element skupa ukupnog prostora ključeva *K*, tada je$\mathrm{P}(k = \{0\}^n) = 0$. Ovo bi značilo da je $\mathrm{P}[K \leftarrow \mathrm{Generate}: \mathrm{Encrypt}(K, m) = m] = 0$ i, samim tim, kriptografski sistem ne bi zadovoljavao definisane zahtjeve jednog savršeno bezbjednog kriptografskog sistema.

Rješenje $k = \{0\}^n$jeste element skupa ukupnog prostora ključeva *K*, ali, ukoliko se desi da ovaj ključ stvarno bude generisan slučajnim procesom, onda se on odbacuje i proces generisanja ključa se ponavlja.

Zapažanje 2. OTP ključevi su komplikovani za generisanje, veliki i upravljanje njima je komplikovano.

Ideja Koristiti isti ključ više puta za kriptovanje različitih poruka

Ovo nije dobra ideja iz sledećeg razloga:

Neka je $c_0 = m_0 \oplus k$ i $c_1 = m_1 \oplus k$

U ovom slučaju imamo:

$c_0 \oplus c_1 = (m_0 \oplus k) \oplus (m_1 \oplus k)$

$= m_0 \oplus (k \oplus m_1 \oplus k)$

$= (m_0 \oplus m_1) \oplus (k \oplus k)$

$= (m_0 \oplus m_1) \oplus 0$

$= (m_0 \oplus m_1)$

Iz gore izvedenih formula vidimo da bi se na osnovu dva kriptograma moglo doći do informacija o pojedinim porukama, a na osnovu toga i do samih poruka i ključa sa kojim se šifruju. Na ovaj način bi se omogućilo dešifrovanje svih budućih kriptograma.

Rješenje Nikad ne koristiti isti ključ dva puta!

Iako je matematički dokazano da je OTP kriptosistem savršeno bezbjedan, u praksi situacija nije tako jednostavna. Naime OTP kriptosistem spada u kategoriju simetričnih kriptografskih sistema i dijeli osnovnu manu ovih sistema, a to je upravljanje ključevima za šifrovanje. Ovaj problem je posebno izražen kod OTP kriptosistema, s obzirom na to da dužina ključa mora biti jednaka dužini poruke i isti ključ se ne smije koristiti dva puta.

Zbog navedenih problema, upotreba OTP kriptosistema nije često zastupljena, a najpoznatiji primjer njegove upotrebe je kripografska mašina Enigma koju su upotrebljavali Nijemci tokom drugog svjetskog rata. Proboj ovog kriptografskog sistema je napravljen kroz presretanje ključa za šifrovanje i otkrivanje algoritma za njegovo kreiranje, a samim tim je omogućeno dešifrovanje kriptograma. Ovo je imalo značajne konsekvence na rezultate drugog svjetskog rata.

5.3 Bezuslovno bezbjedan kriptografski sistem

Bezuslovno bezbjedan kriptografski sistem može se realizovati kombinacijom dva kriptografska sistema:

1. upotrebom kvantne kriptografije. Sa ovim sistemom bi se realizovala potpuno bezbjedna distribucija tajnog ključa i detekcija neovlašćenog nadgledanja komunikacionog kanala;
2. upotrebom OTP kriptografskog sistema. Sa ovim sistemom bi se vršilo šifrovanje podataka koristeći tajni ključ koji je distribuiran na potpuno bezbjedan način u prethodnom koraku.

Ovako realizovan kriptografski sistem je bezuslovno bezbjedan, jer se zasniva na nepromjenjivim fizičkim zakonima i na savršeno bezbjednom kriptografskom sistemu za koji postoji matematički dokaz da je savršeno bezbjedan.

Ova tvrdnja u značajnoj mjeri je zasnovana na pretpostavci da je napravljena savršena tehnička realizacija predmetnih podsistema, što nije jednostavano realizovati. U dijelu realizacije sistema kvantne kriptografije, pred istraživačima stoje značajni izazovi kod kreiranja predajnika koji bi emitovao samo jedan foton i prijemnika koji bi pouzdano primio tako slab signal. Bez obzira na tehnička unapređenja koja budu realizovana, sasvim je jasno da se ovi zahtijevi ne mogu realizovati samo kroz tehničko poboljšanje opreme. Čak i ako uspijemo da napravimo predajnik koji emituje samo jedan foton, jasno je da će ovaj uređaj biti nesavršen i da će povremeno da emituje više fotona. Slična je situacija i na strani prijemnika, koji nikada ne može primati signal u savršenim uslovima, već uvijek imamo i određeni nivo šuma. Da bi se prevazišle tehničke nesavršenosti opreme i uticaj okoline, neophodno je raditi i na poboljšanju postojećih, ili pronalaženju novih algoritama za kvantnu distribuciju ključeva. Kod OTP podsistema, osnovni problem leži u činjenici da dužina tajnog

ključa ne može biti kraća od dužine poruke koja se šifruje. Ovaj problem se može prevazilaziti kroz poboljšanje postojećih ili pronalaženje novih algoritama za kompresiju ili kodiranje podataka, ali i kroz poboljšanje optičke mreže koja se koristi za prenos fotona. Poboljšanom kompresijom podataka smanjuje se količina podataka koju treba šifrovati, pa samim tim, i tajni ključ. Poboljšanjem optičke mreže i postavljanjem kvalitetnijih optičkih vlakana, povećava se kapacitet tj. brzina prenosa podataka i, na taj način, omogućava prenos veće količine podataka u kraćem vremenu. Ovakvim unapređenjima umanjuje se značaj koji ima dužina tajnog ključa, jer se on može generisati veoma često i veoma brzo distribuirati preko kvantnog komunikacionog kanala.

Bez obzira na prezentovane činjenice vezane za probleme tehničke realizacije bezuslovno bezbjednog kriptografskog sistema, ovaj koncept je od izuzetnog značaja jer prvi put postoji prijedlog kriptografskog sistema čija bezbjednost nije zasnovana na kompleksnosti matematičkih operacija, a tehnička realizacija sistema uvijek može da se unapređuje i usavršava.

6 Zaključak

U ovom radu razmatran je uticaj koji Shorov algoritam kvantne faktorizacije ima na savremene kriptografske sisteme, a zbog razvoja kvantnih kompjutera. O značaju problema i njegovoj aktuelnosti mogu da posvjedoče brojni tekstovi koji se mogu pronaći u štampi, ili drugim medijima. Tako, na primjer, u [15] se može pronaći veoma zanimljiv tekst o napretku u izradi kvantnih kompjutera Republike Kine. Slični tekstovi mogu se naći svaki dan na Internetu, a kompanija IBM je u julu 2017. godine objavila da je proizvela kvantne kompjutere sa 16 i 17 qubita. Kvantni kompjuteri trenutno ne postoje kao komercijalni proizvodi, ali je evidentno da su proizvedeni i uspješno testirani. Nije poznat njihov status u smislu ukupnog broja qubita, koje bi morali da imaju, da bi mogli uspješno da faktorizuju velike brojeve koji se danas koriste u praksi. Činjenica da su kvantni kompjuteri uspješno proizvedeni i testirani, neminovno dovodi do zaključka da je uticaj Shorovog algoritma kvantne faktorizacije na bezbjednost osnovnog algoritma asimetrične kriptografije - RSA algoritma, u ovom momentu, veoma veliki. Izvjesno je da su se stvorili uslovi za podršku naučnim istraživanjima koja bi dovela do pronalaženja novih algoritama, otpornih na uticaj kvantnih kompjutera, ili novih kriptografskih sistema koji bi bili bezuslovno bezbjedni.

S dobzirom na iskustva vezana za prethodne periode, jasno je da će jedino prihvatljivi biti kriptografski sistemi za koje će postojati teorijski dokazi da su savršeno bezbjedni (kao što je OTP u ovom momentu), ili kriptografski sistemi zasnovani na dokazanim fizičkim zakonima (kao što je kvantna kriptografija u ovom momentu). U radu je predložena kombinacija dva kriptografska sistema, kvantne kriptografije i OTP, u cilju dobijanja bezuslovno bezbjednog kriptografskog sistema.

Promjena koje donose nove tehnologije opisane u ovom radu se ne treba bojati, jer je izvjesno da će nove tehnologije dovesti do značajnog napretka civilizacije, kao toliko puta u istoriji. Teško je zamisliti koristi koje će društvo imati kroz upotrebu kvantnih kompjutera praktično neograničenih računskih mogućnosti, ili promjene u društvu koje će donijeti bezuslovno bezbjedna komunikacija.

Najbolje od svega je što mi živimo u vremenu kad se ove promjene dešavaju i što lično možemo dati doprinos ovim unapređenjima ili promjenama. Postoji mnogo pravaca u kojima možemo dati doprinos, a ovdje su navedene samo neke preporuke:

- pronalaženje novih tehnika za realizaciju kvantnih kompjutera, ali i rad na otklanjanju uočenih problema koji postoje u interferenciji između kvantnih kompjutera i okoline kod proširivanja broja qubita u kvantnim memorijskim registrima;
- pronalaženje novih protokola koji bi implementirali osnovne funkcionalnosti kvantne kriptografije, ali i rad na usavršavanju postojećih protokola, ili eksperimentalna provjera i potvrda njihove efikasnosti.

Literatura

[1] Arthur Conan Doyle: „The Adventure of the Dancing Men“, Collier's, 05. December, 1903;

[2] Simon Singh: „The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography", Anchor Books, New York, 1999;

[3] Claud Shannon: „Communication Theory of Secrecy Systems“, Bell System Technical Journal, Volume 28, No. 4, Pages 656–715, 1949;

[4] Whitfield Diffie and Martin Hellmann: „New Directions in Cryptography“, IEEE Transactions on Information Theory, Volume 22, Issue 6, Pages 644-654, November 1976;

[5] Ronald Rivest, Adi Shamir, and Leonard Adleman: „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems“, Communications of the ACM,Volume 21, Issue 2, Pages 120-126, February 1978;

[6] Gilbert Vernam: „Cipher printing telegraph system:For secret wire and radio telegraphic communications“, Journal of the A.I.E.E.,Volume 45, Issue 2, Pages109 – 115, February 1926;

[7] Federal Information Processing Standards Publication 197: „Announcing the ADVANCED ENCRYPTION STANDARD (AES)“, 26. November 2001;

[8] Werner Heisenberg: „Ueber den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik.“, Zeitschrift für Physik, Springer Verlag No. 43, Pages172-198, Berlin, 1927;

[9] Debashis Sen: „The uncertainty relations in quantum mechanics“, Current science, Volume 107, No. 2, 25. July. 2014;

[10] Charles Bennett, Gilles Brassard: „Quantum Cryptography: Public key distribution and coin tossing“, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Pages 175 – 179, Bangalore, India, December.1984;

[11] Artur Ekert:„Quantum Cryptography Based on Bell's Theorem", Physical Review Letters. American Physical Society. Volume 67, No. 6, Pages 661–663, 5.August 1991;

[12] Charles Bennett, Gilles Brassard, and Artur Ekert: „Quantum cryptography“, Scientific American, Volume 267, No. 4, Pages 50 – 57, October 1992;

[13] David Deutsch, Artur Ekert and Rossella Lupacchini: „Machines, Logic and Quantum Physics", Bulletin of Symbolic Logic, Volume 6, No. 3, Pages 265-283, 2000;

[14] Michael Nielsen and Isaac Chuang: „Quantum Computation and Quantum Information 10th Anniversary Edition“, Cambridge University Press, New York, 2010;

[15] https://hardware.slashdot.org/story/17/05/03/1958207/china-makes-quantum-leap-in-developing-quantum-computer;

[16] Peter Shor: „Introduction to quantum algorithms“, Proceedings of Symposia in Applied Mathematics (PSAPM), 29. April. 2000;

[17] Artur Ekert and Richard Jozsa: „Quantum computation and Shor’s factoring algorithm“, The American Physical Society Reviews of Modern Physics, Volume 68, No. 3, July 1996;

[18] Peter Shor: „Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer“, Society for Industrial and Applied Mathematics Journal on Computing, Volume 26, No. 5, Pages 1484 – 1509, 1997;

[19] Ivan Niven, Herbert Zukerman, Hugh Montgomery: „An Introduction to the Theory of Numbers Fifth Edition“, John Wiley& Sons, Inc, New York, 1991;

[20] Charles Bennett, Francois Bessette, Gilles Brassard, Louis Salvail, and John Smolin: „Experimental quantum cryptography“, Journal of Cryptology, Volume 5, Issue 1, Pages 3 – 28. January 1992;

[21] Emma Strubell: „An Introduction to Quantum Algorithms“, COS498 – Chawathe Spring, Volume 13, 2011;

[22] Ivan Ordavo: „Free-Space Quantum Cryptography“, Department für Physik München, 16. Juny 2006;

[23] Ms. Deepa Harihar Kulkarni: „Research Directions in Quantum Cryptography and Quantum Key Distribution“, International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012;

[24] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone: „Report on Post-Quantum Cryptography“, National Institute of Standards and Technology, U.S. Department of Commerce, April 2016;

[25] Miloslav Dušek, Norbert Lutkenhaus, Martin Hendrych: „Quantum cryptography“, Progress in Optics, Volume 49, Edition E. Wolf v3, Pages 381-454, 2 May 2006;

[26] Franck Lin: „Cryptography's Past, Present, and Future Role in Society“, https://engineering.wustl.edu/.../ecc/Documents/Lin.pdf, 16.December 2010;

[27] Manindra Agrawal, Neeraj Kayal, Nitin Saxena: „PRIMES is in P”, Department of Computer Science & Engineering Indian Institute of Technology Kanpur, 6. August 2002;

[28] Dario Maltarski: „Sito polja brojeva”, Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, matematički odsjek, Septembar 2014.

[29] Manin, Ivanovitch. Yuri: „Vychislimoe i nevychislimoe“, Soviet Radio 1980;

[30] Paul Benioff: "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines", Journal of Statistical Physics, Volume 22, Issue 5, Pages 563-591 SPRINGER, May 1980;

[31] Paul Benioff: „Quantum-Mechanical Models of Turing Machines That Dissipate No Energy“, Physical Review Letters, Volume 48, No. 23, Pages 1581–1585, June 1982;

[32] Richard P. Feynman: „Simulating Physics with Computers“, International Journal of Theoretical Physics, Voume 21, 1982;

[33] David Deutsch: „Quantum Theory: The Church-Turing Principle and the Universal Quantum Computer“, Proceedings of the Royal Society of London, Series A, Volume 400, No. 1818, Pages 97–117, 1985.