Vrsta rada: Originalni naučni rad
Primljen: 14. 2. 2022.
Prihvaćen: 6. 11. 2022.
UDK:

Zaštita i upravljanje bezbednosnim rizicima, predlog kriptoloških mera i rešenja za preduzeće „Vesimpex"

Ivan Jovanović [1], Milosav Majstorović [1] i Hana Stefanović[1] *

[1] Visoka škola strukovnih studija za informacione tehnologije ITS, Beograd, Srbija; ivan59218@its.edu.rs; milosav.majstorovic@its.edu.rs
* hana.stefanovic@its.edu.rs; +381 (0)63/84-97-189

Sažetak: Predmet istraživanja ovog rada je pravljenje asocijativne mreže pojmova u okviru upravljanja bezbednosti i primena kriptografije kroz sekundarno istraživanje, kao i uočavanje značaja bezbednosti u konkretnoj organizaciji kroz primarno istraživanje. Cilj je da se na osnovu analize preduzeća formuliše predlog bezbednosnih i kriptoloških mera kako bi se unapredio bezbednosni sistem preduzeća. Cilj osnovnih principa informatičke bezbednosti malih i srednjih preduzeća, kao i primene odgovarajućih kriptografskih algoritama zasnovanih na principu jednokratne šifre (OTP – one-time pad) i vizuelne kriptografije (VC – Visual Cryptography), predstavlja kreiranje završnog rešenja za odabrano preduzeće. Rad pored teorijske osnove sadrži i informacije o samom preduzeću sakupljene posmatranjem i beleženjem i analizom sadržaja, kao i proces kreiranja bezbednosnog rešenja inkorporiran u projektnu povelju i samo rešenje.

Ključne reči: mala i srednja preduzeća; bezbednosna rešenja; konkurentska prednost; jednokratna šifra (OTP – one-time pad); vizuelna kriptografija (VC – Visual Cryptography)

1. Uvod

Informatičko doba i digitalizacija doprinose značajnom poboljšanju svih oblika poslovanja, ali su takođe i informacije lako dostupne, što ugrožava bezbednost samog poslovnog sistema [1]. U veoma oštroj konkurentskoj trci na tržištu zaštita informacija postala je neophodna [2], jer postoje različiti upadi, bez obzira na to da li su internog, eksternog ili slučajnog tipa, a sve češće nastaju usled zloupotrebe novih tehnologija [3][4]. Zahvaljujući pouzdanim bezbednosnim sistemima, znatno se smanjuje rizik od curenja informacija [5] koje može da bude fatalno za preduzeće.

„Vesimpex" je malo preduzeće koje se bavi prodajom i ugradnjom elektroopreme, kao i kreiranjem samostalnih rešenja u oblasti elektrodistribucije [6]. Preduzeće sarađuje sa mnogim uspešnim kompanijama u različitim granama industrije, pa pitanje bezbednosti i pouzdanosti informacija sve više dobija na značaju. U takvom okruženju pojačana bezbednost može preduzeću dati prednost u odnosu na konkurenciju, koja je često nelojalna [7]. Kako bi se obezbedila zaštita od raznih napada, potrebno je analizirati postojeće stanje i nivo stručnosti zaposlenih i na osnovu toga dati predlog o formiranju bezbednosnog sistema za posmatrano malo preduzeće.

Predmet istraživanja rada je multidisciplinaran i ulazi u discipline ekonomike preduzeća, upravljanja projektima, bezbednosti i kriptografije. Glavni motiv je formiranje konkretnog rešenja na praktičnom primeru kroz analiziranje bezbednosnih karakteristika preduzeća. Svrha istraživanja je pronalaženje adekvatnih načina za realizaciju formulisanih ciljeva kako bi se omogućila realizacija bezbednosnih kriterijuma.

Glavni cilj ovog primenjenog istraživanja je rešenje specifičnog bezbednosnog problema kroz kreiranje bezbednosnog rešenja i obezbeđenje konkurentske prednosti za preduzeće „Vesimpex" [6]. Pomoćni ciljevi su proučavanje postojećih i uvođenje novih mera kriptološke zaštite radi povećanja bezbednosti poslovanja.

S obzirom na to da je savremeno poslovanje, koje se pre svega zasniva na upotrebi računarskih sistema i razmeni podataka u elektronskom obliku, izloženo različitim rizicima koji mogu imati nesagledive posledice, neophodno je analizirati i sprečiti sve učestalije napade na računarske mreže, pokušaje neovlašćenog pristupa podacima, prisluškivanja, kao i zlonamerne izmene podataka [8]. U tom smislu, neophodno je primeniti nove načine komunikacije koje napredak tehnologije omogućava. Problem sigurnosti nameće potrebu za uvođenjem novih mehanizama koji treba da preuzmu ulogu klasičnih rešenja sa ciljem efikasne identifikacije, kontrole pristupa i verifikacije. Odgovor na većinu ovakvih izazova nudi primena kriptografskih rešenja [9], mada postoje i problemi na koje kriptografija ne može adekvatno da odgovori.

Kriptografija izučava različite tehnike transformacije podataka koji se prenose na takav način da značenje podataka bude dostupno samo ovlašćenim stranama u komunikaciji. Istovremeno, transformacija treba da bude takva da neovlašćene strane u komunikaciji koje dođu u posed transformisane poruke ne mogu da dođu do polaznih podataka.

Postoji veliki broj kriptografskih algoritama, klasičnih i modernih, a takođe i onih koji koriste isti ključ za šifrovanje i dešifrovanje, kao i nesimetričnih, koji koriste različite ključeve u procesu šifrovanja i dešifrovanja. Za svaku od kriptografskih šifara, bez obzira na to da li se koristi simetričan ili nesimetričan kriptografski algoritam, ključno je pitanje sigurnosti šifre [10] [11].

Pod bezuslovno sigurnom šifrom se smatra ona šifra koja ima osobinu da se ne može doći do otvorenog teksta iz šifrata bez poznavanja ključa, čak ni potpunom pretragom ključeva. Sigurno je da se potpunom pretragom (ne ograničavajući vreme pretrage i raspoložive resurse) može doći do ključa, ali napadaču nije od interesa da to bude urađeno nakon nekoliko desetina ili stotina godina. Međutim, ukoliko bi napadač posedovao najbolju moguću opremu i resurse, bezuslovno sigurna šifra treba da omogući da on ne dođe u posed otvorenog teksta ni pri idealizovanim uslovima. Osnovna ideja bezuslovno sigurne šifre je da se potpunom pretragom potencijalnih ključeva, koji svakako generišu veliki broj poruka, učini da napadač nema načina da odredi koja je od njih prava. Napadač će potpunom pretragom dobiti veliki broj besmislenih poruka, koje će odbaciti, ali će svakako dobiti i određeni broj smislenih, a ako su sve te poruke podjednako verovatne, onda napadač nema načina da odredi koja je od njih prava.

Primer bezuslovno sigurne šifre je one-time pad – OTR šifra [12], koja je primenjena u ovom radu. Simulacioni modeli koji prikazuju osnovne principe OTP algoritma realizovani su u softverskom alatu CrypTool [13], sa posebnim osvrtom na slučaj ponovljene upotrebe ključa koji je predviđen za jednokratnu upotrebu. Priložen je i jedan primer procesiranja elektronske finansijske transakcije primenom OTP-a, uz deljenje tajnih informacija primenom tehnike virtuelne kriptografije [14][15].

2. Materijali i metode

Tokom izrade korišćeni su brojne naučne i stručne metode, tehnike i alati, a plan istraživanja obuhvata:

- definisanje predmeta istraživanja (kroz formulaciju problema istraživanja);
- definisanje ciljeva istraživanja;
- pregled relevantne literature i njen izbor za istraživanje;
- određenje teorijskog okvira istraživanja (u skladu sa zastupljenim disciplinama i izborom relevantne literature);
- situaciona analiza;
- ispitivanja ciljne grupe kroz anketno istraživanje;
- statistička analiza podataka anketnog istraživanja;
- osmišljavanje i izrada bezbednosnog rešenja.

Glavna hipoteza istraživanja:
H1: Nivo informatičke bezbednosti u preduzeću „Vesimpex" nije optimalan, te ga je, s obzirom na elemente okruženja i željeni rast i razvoj kao organizacioni cilj, potrebno unaprediti novim bezbednosnim rešenjem.
H2: Ako bi se adekvatno unapredila informatička bezbednost preduzeća, to bi mu obezbedilo konkurentsku prednost.

Ishodi istraživanja, odnosno očekivani rezultati istraživanja su: analiza odabranih bibliotečkih i drugih referentnih izvora, dokazivanje postavljenih hipoteza i rešavanje centralnog problema istraživanja kroz odabrani model. Sa stanovišta stručne opravdanosti, rešenje koje je predloženo dodatno bi unapredilo poslovanje i bezbednost posmatranog preduzeća, poboljšalo sigurnost poslovanja, kao i sigurnost uključenih partnera (dobavljača, klijenata). Društvena opravdanost istraživanja leži u podizanju svesti o značaju bezbednosti informacija i u optimizaciji nivoa bezbednosti podataka domaćih preduzeća.

3. Rezultati

Rezultati prezentovani u ovom poglavlju predstavljaju konkretno rešenje za bezbednosni sistem preduzeća, koji, iako je na prihvatljivom nivou, ima dosta prostora za unapređenje. Glavne nadgradnje predložene su na polju vršenja transakcija i skladištenja poverljivih informacija, kao što su lozinke zaposlenih.

Nakon što je obezbeđen siguran kanal i način prenosa poverljivih informacija, dat je predlog da se poverljivim podacima, kao što su lozinke zaposlenih, pre određivanja heš vrednosti doda slučajna salt vrednost, kako bi se postigla dodatna zaštita u slučaju napada.

3.1. Deljenje tajnih informacija prilikom vršenja transakcija

U slučaju vršenja elektronskih finansijskih transakcija primenjena je tehnika proširivanja piksela originalne digitalne slike, čiji je sadržaj jednokratni PIN kod. Procesi šifrovanja i dešifrovanja su relativno jednostavni i imaju visoku sigurnost, jer se predložena tehnika vizuelne kriptografije oslanja na one-time pad algoritam.

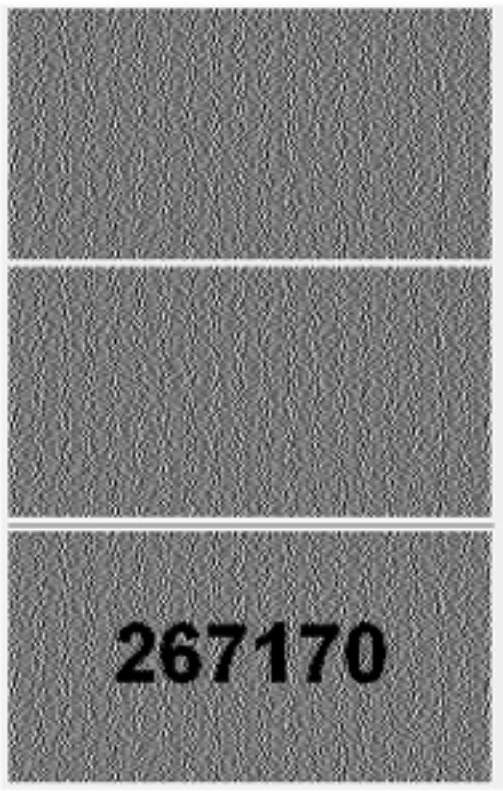
Vizuelna kriptografija predstavlja kriptološku tehniku koja omogućava skrivanje informacija, odnosno tajnih poruka, na takav način da one mogu biti dešifrovane na mestu prijema bez upotrebe računara ili bilo kakvih drugih izračunavanja [12]. U postupku dešifrovanja koristi se samo ljudski vizuelno-perceptivni sistem. Ova tehnika predložena je prvi put na EUROCRYPT konferenciji (Noni Naor i Adi Šamir). Procesi šifrovanja i dešifrovanja su relativno jednostavni i imaju visoku sigurnost, a imaju primenu u deljenju različitih vrsta informacija, naročito u finansijskim transakcijama preko interneta, kao i prilikom provere glasačkih listića, obveznica i sl.

Algoritam deljenja originalne slike na slojeve (share images) realizovan je u Visual Studio C# programskom okruženju. Oba sloja su iste rezolucije i njihovim preklapanjem očitava se tajna poruka [16]. Izabrana je jednostavna varijanta proširivanja piksela koja se vrši slučajnim generisanjem na jednom sloju, dok drugi sloj sa komplementarnim pikselima nakon vizuelnog XOR-ovanja sa prvim (primenom operacije ekskluzivno ILI – XOR) daje informaciju (tajnu poruku) nakon preklapanja.

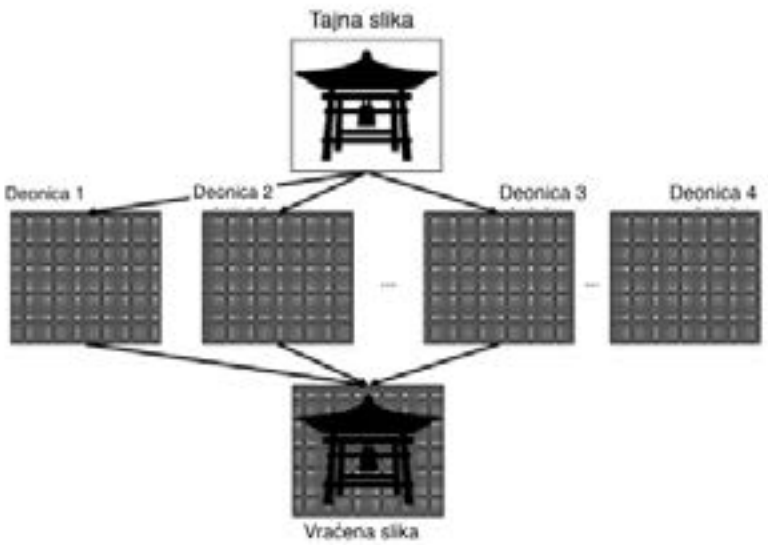
S obzirom na to da su vrednosti kojima su predstavljeni pikseli na prvom sloju slučajno generisane, ova tehnika se može posmatrati kao jedna varijanta one-time pad šifrovanja, koj ima dobre sigurnosne karakteristike.

Transparentne slike (sloj 1 i sloj 2) prikazane su na slici 1, pri čemu prvi sloj sadrži slučajno generisane proširene vrednosti piksela i ta slika predstavlja ključ. Svaki piksel predstavljen je blokom u kojem uvek postoji isti broj belih i crnih piksela. Ukoliko se vrši jednostavniji model ekspanzije piksela, piksel će biti prezentovan jednim belim i jednim crnim pikselom, a ukoliko se koristi složeniji model ekspanzije, piksel će biti predstavljen sa četiri nova piksela, od kojih su dva bela i dva crna. Piksel u sloju 1 ima određeno stanje, a piksel u sloju 2 može imati isto ili suprotno stanje. Ako su stanja u sloju 1 i sloju 2 ista, preklapanjem se dobija polovina belih i polovina crnih piksela, što će ljudsko oko detektovati kao neku nijansu sivog, a ako su stanja u sloju 1 i sloju 2 suprotna, preklapanjem se dobijaju crni pikseli, što će ljudsko oko detektovati kao crno. Preklapanjem ■□ sa istim takvim blokom u sloju 2 dobija se svetli piksel (nijansa sivog), dok se preklapanjem ■□ sa □■ dobija crni piksel. Slično je i u slučaju proširenja blokom od četiri piksela za svaki originalni piksel: preklapanjem ■■ sa istim takvim takvim blokom u sloju 2 dobija se nijansa sivog, a preklapanjem ■■ sa ■■ dobija se crni blok. Sloj 1 sadrži piksele čije su vrednosti određene na slučajan način, što je identično postupku generisanja ključa za one-time pad šifru, dok sloj 2 sadrži fiksne blokove koji su nosioci informacije u fazi preklapanja. Rezultat preklapanja slojeva prikazan je na slici 1, ispod sloja 1 i 2.

Postoje i složenije šeme u vizuelnoj kriptografiji, dok neke od njih ne uključuju model proširivanja piksela, u smislu predstavljanja originalnog piksela grupom subpiksela, ili uključuju dodatne tehnike poboljšanja kontrasta dekodovane slike [17] [18]. Primer upotrebe većeg broja generisanih slojeva na osnovu kojih se dobija dekodovana slika prikazan je na slici 2.



Slika 1. Dobijanje dekodovane slike na osnovu slojeva 1 i 2



Slika 2. Dobijanje dekodovane slike na osnovu četiri sloja (deonice)

3.2. Prikaz osnovnih principa one-time pad algoritma

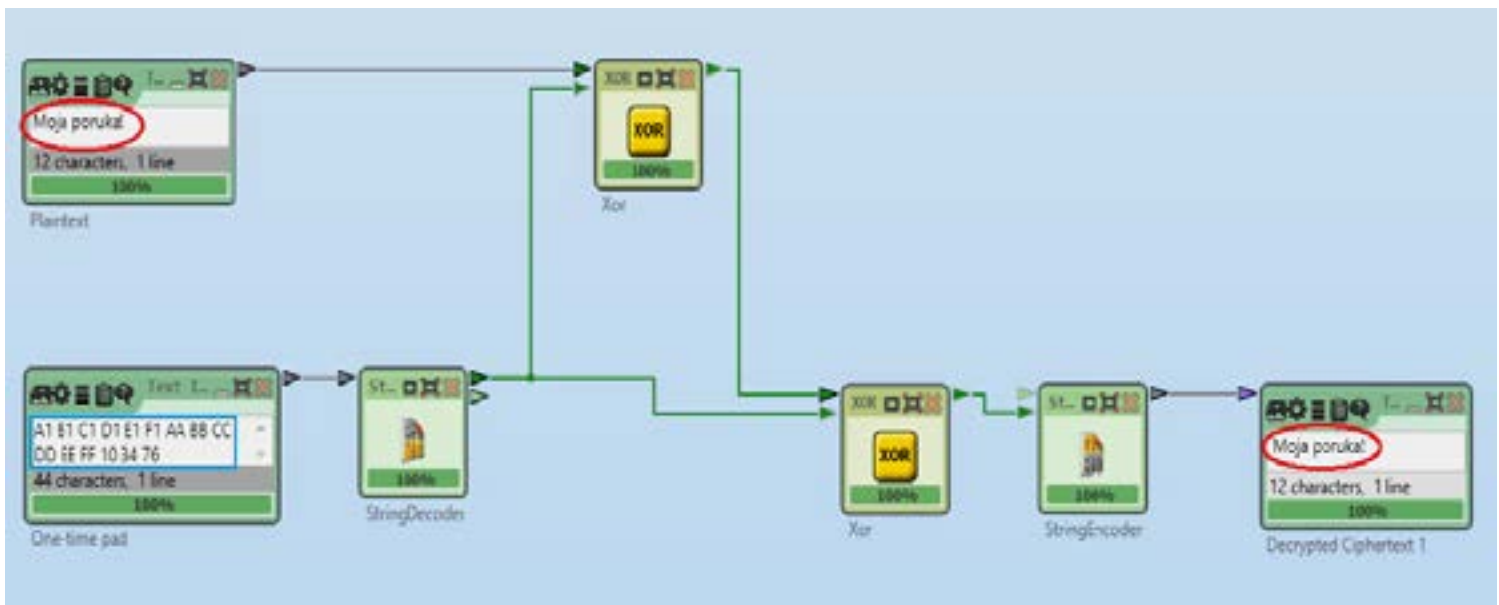
Pre postupka šifrovanja potrebno je poruku predstaviti binarnim nizom na osnovu definisanog koda. Nakon toga je neophodan drugi binarni niz, koji je iste dužine kao i sama poruka, koji će predstavljati ključ. Taj niz treba da ima osobine slučajnog niza. Postupak šifrovanja podrazumeva da se svaki bit otvorenog teksta p_i sabira po modulu 2 (operacija XOR) sa po jednim bitom ključa k_i da bi se dobio odgovarajući bit šifrata c_i [8][19]:

$$c_i = p_i \oplus k_i \quad (1)$$

U postupku dešifrovanja svaki bit šifrata sabira se po modulu 2 sa istim bitom ključa koji je korišćen pri šifrovanju, što, s obzirom na osobine XOR operacije, daje originalni tekst:

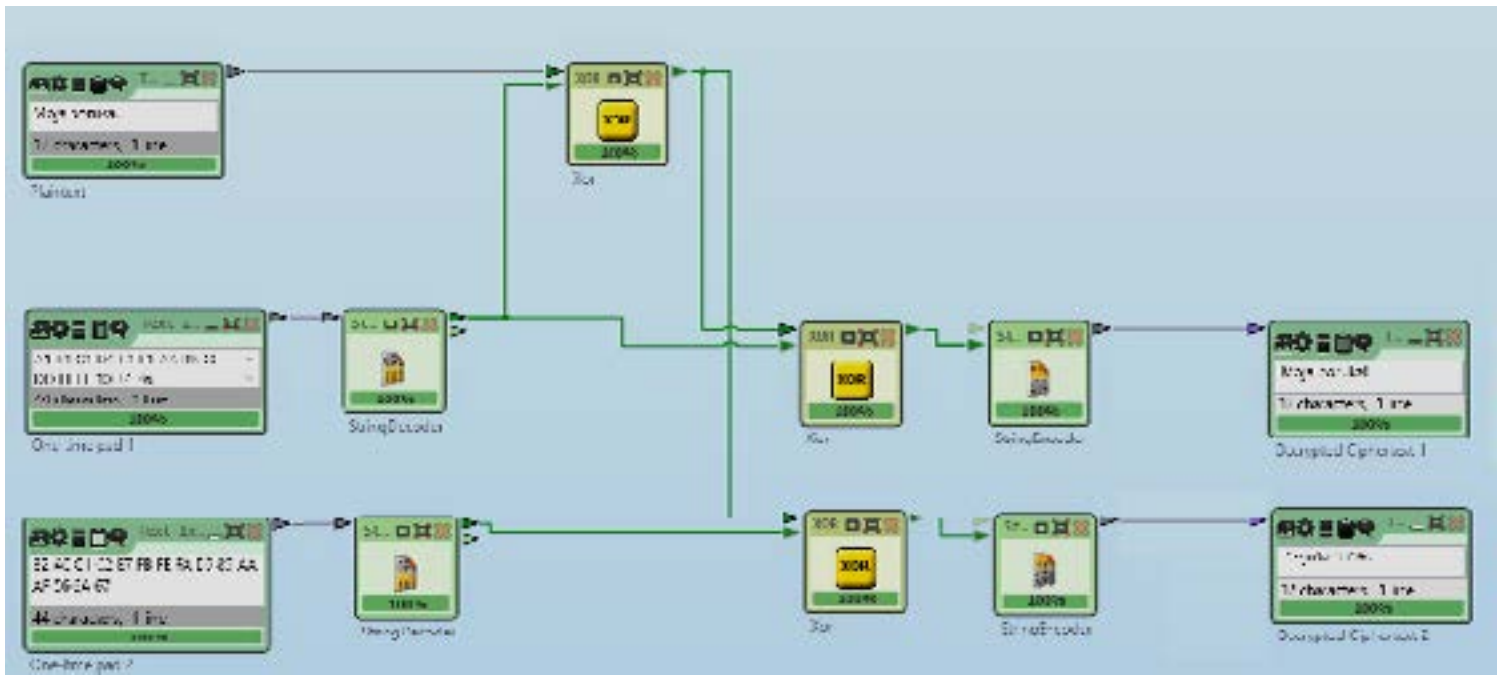
$$p_i = c_i \oplus k_i \quad (2)$$

Simulacioni model, kreiran u softverskom alatu CrypTool, koji prikazuje postupak šifrovanja i dešifrovanja otvorenog teksta (sadržaja „Moja poruka!") primenom OTP-a, prikazan je na slici 3. Ključ koji je korišćen zapisan je u heksadecimalnom formatu u donjem levom uglu, dok je dešifrovana poruka prikazana u donjem desnom uglu.



Slika 3. Simulacioni model koji prikazuje postupak šifrovanja i dešifrovanja otvorenog teksta (sadržaja „Moja poruka!") primenom OTP-a

Pretragom potencijalnih ključeva napadač generiše veliki broj poruka, od kojih će neke biti besmislene, kao što je prikazano na slici 4. Napadač će ovakve poruke odbaciti, ali će sigurno generisati i određeni broj smislenih poruka. Ako su sve te poruke podjednako verovatne, onda napadač nema načina da odredi koja je od njih prava.



Slika 4. Simulacioni model koji prikazuje postupak pretrage potencijalnih ključeva

Sigurnost OTP algoritma zasniva se na slučajnosti ključa. Za pojam slučajnosti ne postoji egzaktna definicija, ali su sa kriptografske strane neophodne dve osnovne karakteristike binarnog slučajnog ključa:

» nepredvidljivost: bez obzira na broj bita ključa koji su poznati, verovatnoća da se pogodi sledeći bit ne sme biti veća od ½. Šansa da sledeći bit bude 1 ili 0 tačno je jednaka ½;
» balansiranost: broj jedinica i nula mora biti približno jednak, u nizu dovoljno velike dužine.

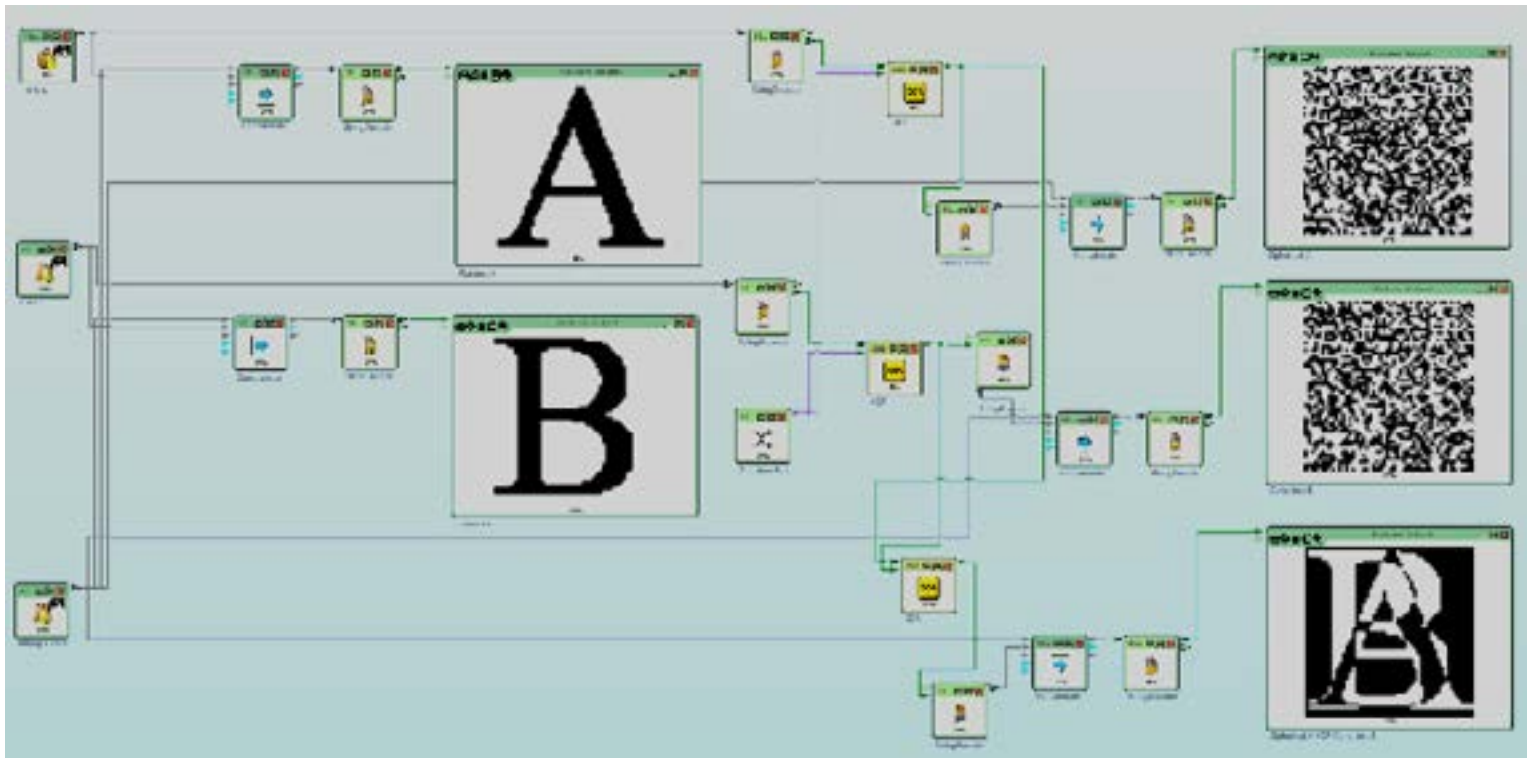
3.3. Slabosti algoritma usled višestruke upotrebe istog ključa

Ako je ključ slučajni binarni niz, onda je verovatnoća da bilo koji bit ključa ima vrednost logičke jedinice jednaka verovatnoći da taj bit ima vrednost logičke nule i iznosi ½. Za razliku od toga, otvoreni tekst ima određene statističke osobine i verovatnoća pojave logičkih jedinica i nula nije jednaka.

Simulacioni model koji ilustruje primenu istog OTP ključa u postupku šifrovanja dve različite poruke prikazan je na slici 5. Kao otvoreni tekst izabrana je digitalna slika da bi se i vizuelno prikazale posledice višestruke primene istog OTP ključa. Ukoliko se izvrši XOR operacija nad šifratima CA i CB, dobija se rezultat:

$$C_A \oplus C_B = (A \oplus K) \oplus (B \oplus K) = (A \oplus B) \oplus (K \oplus K) = (A \oplus B) \oplus 0 = A \oplus B \quad (3)$$

Posledica ove osobine je da inventivni napadač, nakon vršenja XOR operacije nad šifratima, iako napadaču nije poznat ključ K, otkriva dosta o originalnim porukama, što je razlog zbog kojeg višestruka upotreba istog OTP ključa nije preporučljiva. Rezultat prikazan u donjem desnom uglu na slici 5 dosta otkriva o originalnim slikama, što je posledica navedenih osobina XOR operacije [20].

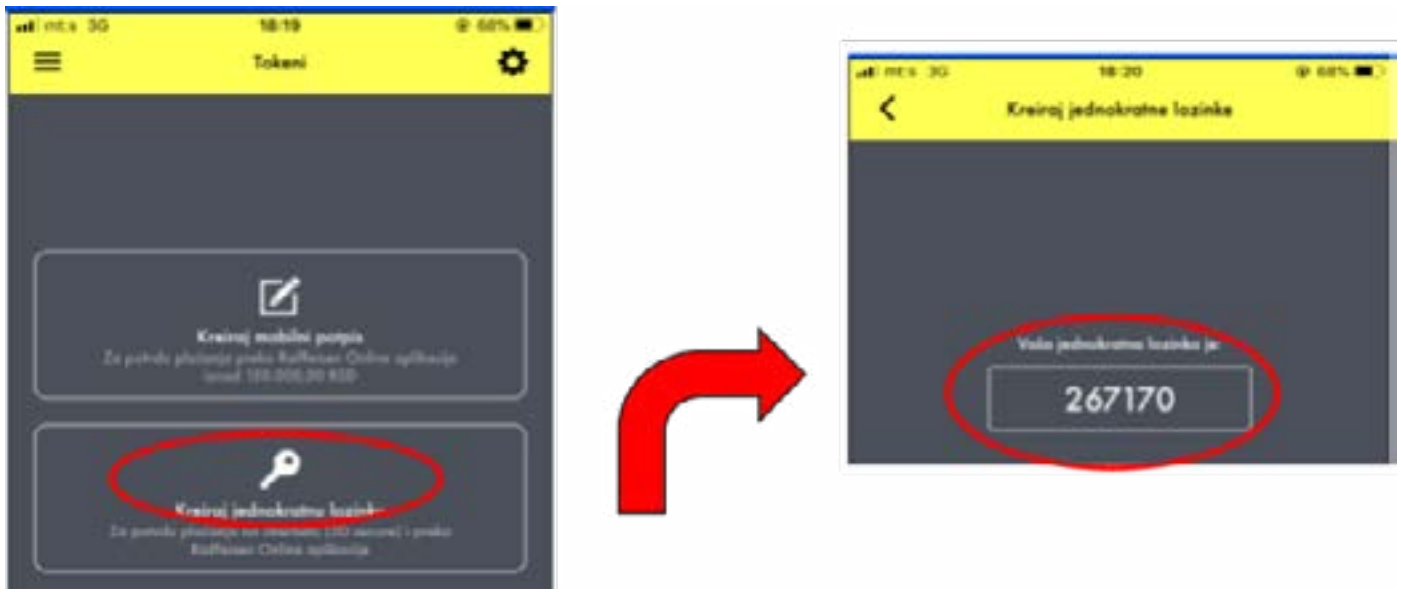


Slika 5. Simulacioni model koji ilustruje višestruku primenu istog OTP ključa

3.4. Primer vršenja elektronskih finansijskih transakcija primenom OTP algoritma

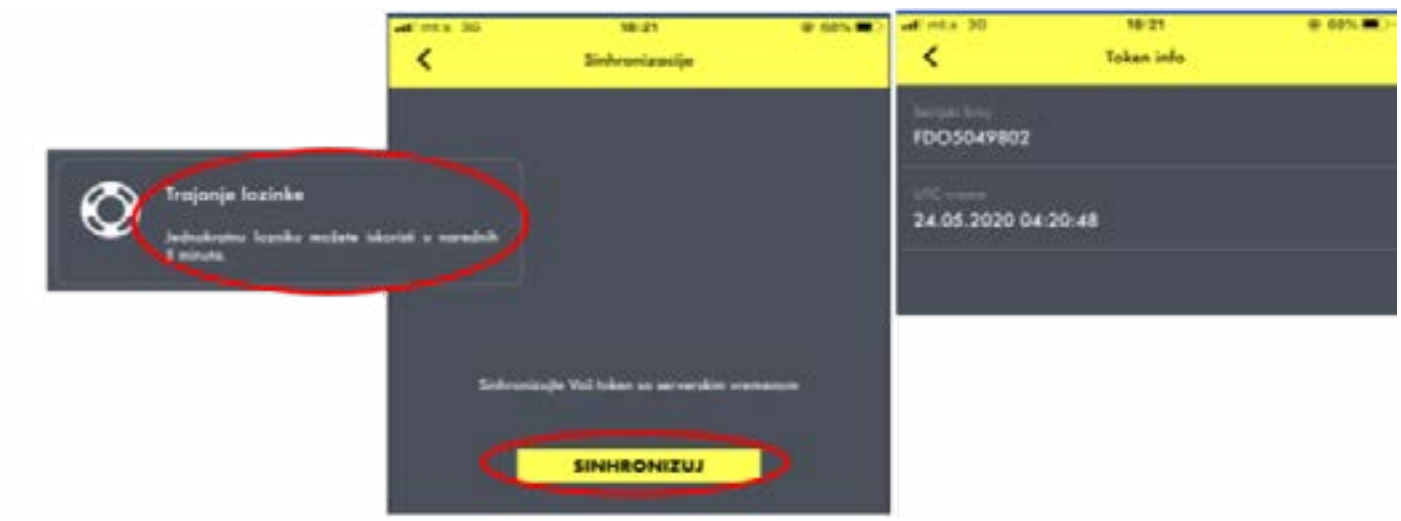
Za prijavu na e-banking aplikacije, koje se vrlo često koriste u poslovnim i privatnim finansijskim transakcijama, potreban je samo serijski broj tokena ili m-tokena. Korisnik nikom ne otkiva svoj PIN za token ili m-token, dok je podrazumevana preporuka da se PIN ne drži uz token ili m-token.

Banka od korisnika ne traži jednokratnu lozinku ni podatak za potpisivanje transakcije [21]. Kreiranje zahteva za generisanje jednokratne lozinke prikazano je u levom delu na slici 6, dok je generisana lozinka poslata na mobilni uređaj korisnika prikazana u desnom delu.



Slika 6. Kreiranje zahteva za generisanje jednokratne lozinke i slanje lozinke na mobilni uređaj korisnika

Podatak o vremenskom važenju lozinke takođe se prosleđuje korisniku, kao što je prikazano na slici 7, uključujući i neke dodatne informacije o tokenu. Trajanje lozinke, prosleđeno korisniku nakon izvršene sinhronizacije sa serverskim vremenom, prikazano je u levom delu na slici 7 i iznosi 5 minuta. Dodatne informacije o tokenu (Token info) koje prikazuju serijski broj i UTC vreme nalaze se u desnom delu na slici 7.



Slika 7. Prikaz podatka o vremenskom važenju lozinke

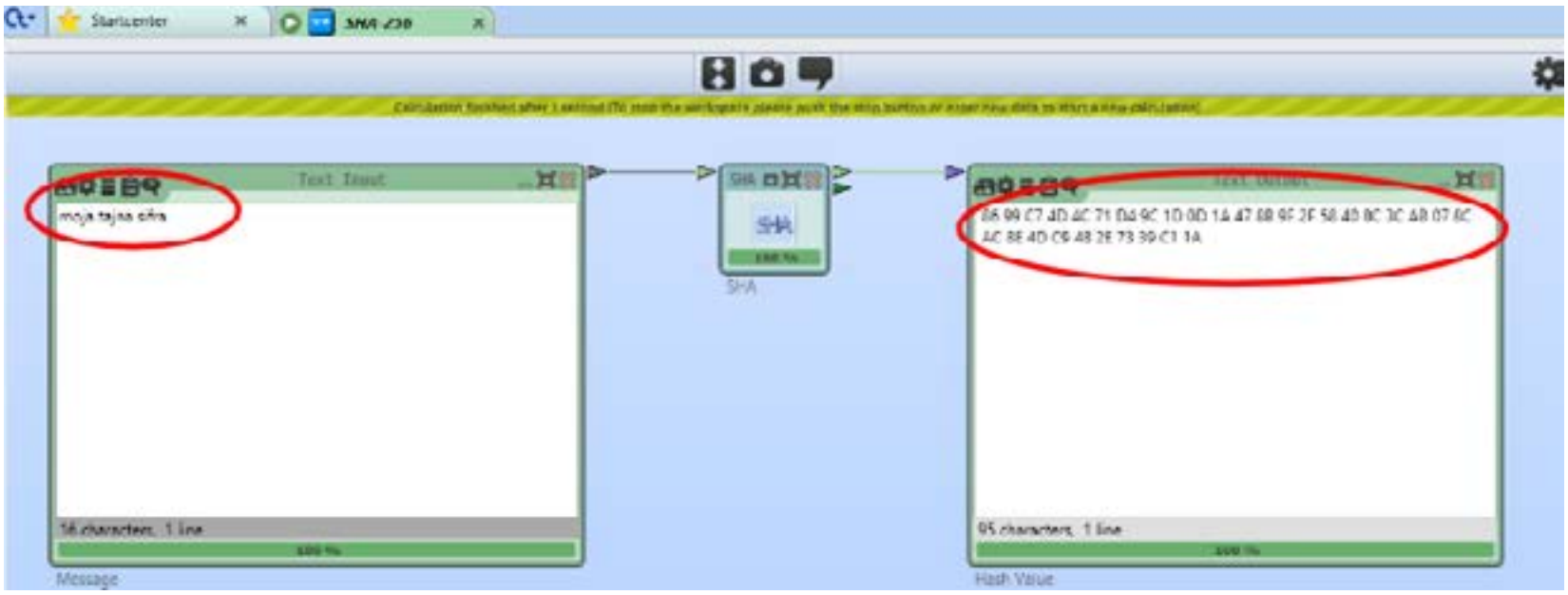
3.4. Predlog čuvanja lozinki zaposlenih primenom heš funkcija i dodavanjem slučajne salt vrednosti

Nakon što je obezbeđen siguran kanal i način prenosa poverljivih informacija, neophodno je čuvati lozinke na način koji sprečava da ih napadač dobije čak i ako je aplikacija ili baza podataka ugrožena. Većina modernih jezika i frejmvorka pruža ugrađenu funkcionalnost za bezbedno čuvanje lozinki.

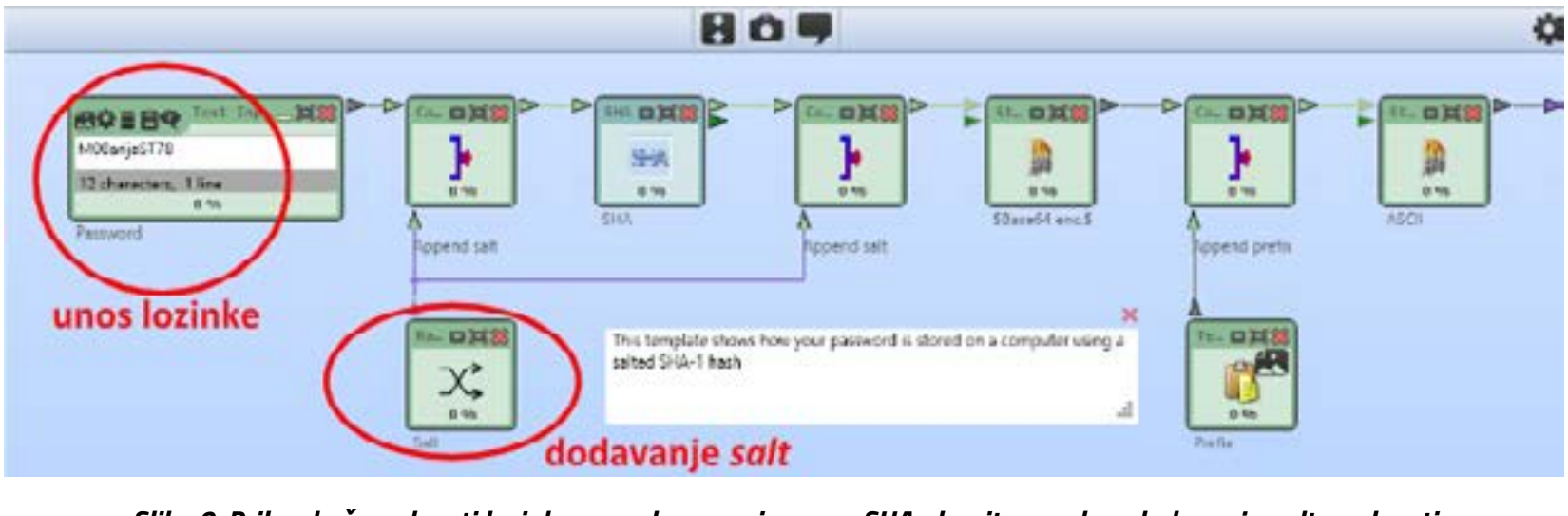
Heširanje i šifrovanje predstavljaju načine za čuvanje osetljivih podataka. Međutim, u gotovo svim okolnostima lozinke je poželjno čuvati u obliku heš vrednosti, a ne kao šifrovane podatke [22]. Heš funkcija je jednosmerna funkcija, što podrazumeva da je praktično nemoguće na osnovu heš vrednosti dobiti originalnu informaciju. Ukoliko bi napadač došao u posed heš vrednosti lozinke, ne bi mogao da na osnovu toga dođe do originalnog podatka, odnosno sadržaja lozinke. U starijim heš algoritmima, kao što je MD5, pronađene su kolizije, i preporuka je primenjivati algoritme novijih generacija (novije generacija SHA).

Kriptografska heš funkcija je jednosmerna funkcija koja za ulazni podatak (poruka, fajl...) proizvoljne konačne dužine kao izlaznu vrednost daje niz fiksne dužine. Osim kompresije kao odlike, heš funkcija mora biti i efikasna, jednosmerna i otporna na kolizije.

Primena SHA algoritma prilikom određivanja heš vrednosti lozinke (sadržaja „moja tajna šifra") prikazana je na slici 8, dok je model koji uključuje dodavanje slučajne salt vrednosti prikazan na slici 9. Modeli prikazani na slici 8 i slici 9 kreirani su u CrypTool softverskom alatu.



Slika 8. Prikaz heš vrednosti lozinke zaposlenog, primenom SHA algoritma



Slika 9. Prikaz heš vrednosti lozinke zaposlenog, primenom SHA algoritma nakon dodavanja salt vrednosti

4. Diskusija

Poboljšanja bezbednosti poslovanja preduzeća „Vesimpex" predložena su u vršenju procesa elektronskih finansijskih transakcija i u postupku skladištenja poverljivih informacija, kao što su lozinke zaposlenih.

Tokom vršenja transakcije primenjena je tehnika proširivanja piksela radi deljenja tokena prilikom generisanja jednokratne lozinke. Procesi šifrovanja i dešifrovanja su relativno jednostavni i imaju visoku sigurnost, jer se oslanjaju na one-time pad tehniku.

Predlog čuvanja pristupnih lozinki zaposlenih uključuje dodavanje slučajne salt vrednosti pre heširanja. Salt vrednosti predstavljaju jedinstvene nasumično generisane nizove koji se dodaju svakoj lozinki i jedinstveni su za svakog korisnika.

Svrha opisanog procesa je da u slučaju upada poverljiva informacija potencijalnom hakeru bude potpuno nerazumljiva i samim tim neupotrebljiva. Na taj način se veći deo odgovornosti za rizik curenja podataka prenosi sa ljudskog faktora na sam bezbednosni sistem, što značajno poboljšava sigurnost poslovanja preduzeća.

Reference

1. Crovini C. Risk management in small and medium enterprises. Routledge; 2019.
2. Hughes P, Ferrett E. Introduction to Health and Safety at Work. 6th ed. New York: Routledge; 2016.
3. Hughes P, Ferrett E. Business Intelligence and Analytics in Small and Medium Enterprises. Melo PN, Machado C, editors. Boca Raton, FL : CRC Press/ Taylor & Francis Group, 2020. | Series: Manufacturing design and technology series: CRC Press; 2018.
4. Ranković M, Ilić M. Upravljanje projektima. Beograd: ITS – Beograd; 2018.
5. Seo JH. Information Security and Cryptology – ICISC 2019: 22nd International Conference, Seoul, South Korea, December 4–6, 2019, Revised Selected Papers. In: Seo JH, editor. Cham: Springer International Publishing; 2020 [cited 2022 Feb 14]. Available from: https://link.springer.com/conference/icisc
6. https://www.vesimpex.rs/ [Internet]. [cited 2022 Feb 14]. Available from: https://www.vesimpex.rs/
7. Ilić M. Osnove ekonomije, finansija i računovodstva. Beograd: ITS-Beograd; 2017.
8. Kumar V, Sharma A, Ntroduction I, August IJ-. A Survey on Various Most Common Encryption Techniques. Int J Adv Res Comput Sci Softw Eng [Internet]. 2014 [cited 2022 Feb 14];3:307–12. Available from: https://www.ijettcs.org/Volume3Issue4/IJETTCS-2014-08-25-137.pdf
9. Menez J., van Oorschot P., Vanstone S. A Handbook of Applied Cryptography. 5th edition. CRC press Series on Discrete Mathematics and Its Applications; 2001.
10. Klima RE, Sigmon NP. Cryptology Classical and Modern. 2nd ed. Chapman and Hall/CRC; 2019.
11. Stallings W. Cryptography and Network Security: Principles and Practice. 3rd ed. Prentice Hall; 2002.
12. Manucom EMM, Gerardo BD, Medina RP. Analysis of Key Randomness in Improved One-Time Pad Cryptography. 2019 IEEE 13th Int Conf Anti-counterfeiting, Secur Identif [Internet]. IEEE; 2019. p. 11–6. Available from: https://ieeexplore.ieee.org/document/8925173/
13. https://www.cryptool.org/en/ [Internet]. Available from: https://www.cryptool.org/en/
14. Ateniese G, Blundo C, Santis A De, Stinson DR. Extended capabilities for visual cryptography. Theor Comput Sci [Internet]. 2001;250:143–61. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0304397599001279
15. Ibrahim DR, Teh J Sen, Abdullah R. An overview of visual cryptography techniques. Multimed Tools Appl [Internet]. 2021;80:31927–52. Available from: https://link.springer.com/10.1007/s11042-021-11229-9
16. Gnanaguruparan M, Kak S. Recursive Hiding of Secrets in Visual Cryptography. Cryptologia [Internet]. 2002;26:68–76. Available from: http://www.tandfonline.com/doi/abs/10.1080/0161-110291890768
17. Askari N, Heys HM, Moloney CR. An extended visual cryptography scheme without pixel expansion for halftone images. 2013 26th IEEE Can Conf Electr Comput Eng [Internet]. IEEE; 2013. p. 1–6. Available from: https://ieeexplore.ieee.org/document/6567726
18. Gonzalez RC, Woods RE. Digital Image Processing Third Edition. 3rd ed. New York: Upper Saddle River, NJ: Prentice Hall; 2008.
19. Dent AW, Mitchell CJ. User's guide to cryptography and standards [Internet]. Boston: Artech House; 2005. Available from: https://pure.royalholloway.ac.uk/portal/en/publications/users-guide-to-cryptography-and-standards(2bda27a3-da21-4407-b057-66c80213c16b).html
20. Stefanovic H, Savic A, Veselinovic R, Bjelobaba G. An application of visual cryptography scheme with digital watermarking in sharing secret information from car number plate digital images. Int J Eng Invent [Internet]. 2021;10:1–11. Available from: www.ijeijournal.com
21. https://www.raiffeisenbank.rs/token/ [Internet]. Available from: https://www.raiffeisenbank.rs/token/
22. Islam MS. Using ECG signal as an entropy source for efficient generation of long random bit sequences. J King Saud Univ - Comput Inf Sci [Internet]. 2022; Available from: https://linkinghub.elsevier.com/retrieve/pii/S1319157822000015