NON - STANDARD SUBSTITUTIONAL CRYPTOGRAPHIC CODES

Melisa Azizovic
Department of Computer Science, University of Novi Pazar, Serbia, melisa.azizovic@gmail.com
Emrus Azizovic
University of Novi Pazar, Serbia, e.azizovic@uninp.edu.rs

Abstract: Modern technologies that involve some form of communication, such as mobile phones, the Internet, digital television, ATMs, generally use codes to ensure security and privacy. The paper deals with the analysis of non-standard substitution codes. The aim of the paper is to show that today cryptosystems play a crucial role in modern technology and to describe the cryptanalysis of non-standard substitution codes. In the first part, we listed the definitions and basic terms that are necessary for successful monitoring of the content of the work. We defined the concept of substitution code and showed with examples how to encrypt and decrypt text using various types of codes. We have described the Pigpen cipher, the Polybius square, and random substitution ciphers. In order to meet the set goals, we used the deduction method, the induction method, the historical method, the causal inference method, the experimental method, as well as the analysis and synthesis methods.
The results of this and similar research indicate that there is a huge interest and necessity for the expansion and improvement of cryptographic models, because today cryptosystems are crucial for modern technology, i.e. technology that involves communication relies on codes to ensure security and privacy. After this basic analysis, a more extensive analysis of other polyalphabetic substitution codes is planned. As well as improving the implementation of proposed solutions in the field of substitution codes in those models. The proposed methods are explained in detail and supported by concrete examples
Keywords: Cryptography, Substitution code, Pigpen code, Polybius square, random substitution codes.

NESTANDARDNE SUPSTITUCIJSKE KRIPTOGRAFSKE ŠIFRE

Melisa Azizović
Departman za računarske nauke, Univerzitet u Novom Pazaru, Srbija, melisa.azizovic@gmail.com

Emruš Azizović
Univerzitet u Novom Pazaru, Srbija, e.azizovic@uninp.edu.rs

Rezime: Savremene tehnologije koje podrazumevaju neki vid komunikacije, kao što su mobilni telefoni, internet, digitalna televizija, bankomati, uglavnom koriste šifre kako bi se osigurala bezbednost i privatnost. Rad se bavi analizom nestandardnih supstitucijskih šifri. Cilj rada je ukazati da danas kriptosistemi igraju presudnu ulogu u modernoj tehnologiji i opisati kriptoanalizu nestandardnih supstitucijskih šifri. U prvom delu smo naveli definicije i osnovne pojmove što je neophodno za uspešno praćenje sadržaja rada. Definisali smo pojam supstitucijske šifre i na primerima pokazali kako se šifrira i dešifrira tekst korišćenjem raznih tipova šifri. Opisali smo Pigpen šifru, Polybiusov kvadrat i nasumične supstitucijske šifre. Kako bi odgovorili na postavljene ciljeve, koristili smo metodu dedukcije, metodu indukcije, istorijsku metodu, metodu kauzalnog zaključivanja, eksperimentalnu metodu, kao i metode analize i sinteze.
Rezultati ovog i sličnih istraživanja ukazuju da postoji ogromna zainteresovanost i neophodnost za širenje i usavršavanje kriptografskih modela, jer danas kriptosistemi su presudni za modernu tehnologiju tj. tehnologiju koja podrazumeva komunikaciju oslanja se na šifre da bi se osigurala bezbednost i privatnost. Posle ove osnovne analize u planu je opširnija analiza ostalih polialfabetskih supstitucijskih šifri. Kao i unapređenje implementacije predloženih rešenja u oblasti supstitucijskih šifri u tim modelima.Predložene metode su detaljno objašnjene i potkrepljene konkretnim primerima.
Ključne reči: Kriptografija, Supstitucijske šifre, Pigpen šifra, Polybiusov kvadrat, nasumične supstitucijske šifre,.

1. UVOD

Kroz celu istoriju čovečanstva uvek je postojala potreba za bezbednom komunikacijom. Još su se stari Egipćani i Indijci bavili problemom bezbednosti. "Kriptografija je prevođenje razumljivog teksta (jasan tekst, otvoreni tekst), ili bilo kojeg drugog skupa podataka, u nerazumljiv tekst (kriptovani tekst, kriptogram ili šifrat), kako bi ga na taj način jedino onaj koji poseduje unapred utvrđen ključ za razumevanje (dešifriranje) mogao prevesti u izvorni, razumljiv tekst" (Dujella i Maretić, 2007).

Cilj rada je ukazati da danas kriptosistemi imaju značajnu ulogu u savremenoj tehnologiji. Tehnologije koje podrazumevaju komunikaciju, kao što su mobilni telefoni, bankomati, internet, digitalna televizija, koriste šifre da bi si osigurala bezbednost i privatnost.

Takođe, cilj rada je opisati kriptoanalizu nestandardnih supstitucijskih šifri. Kod supstitucijskih šifri, redosled slova ostaje isti, stim što se za svako slovo supstituiše nekim drugim slovom, ili nekim drugim simbolom. Na taj način nastale šifre nazvane su kao supstitucijske jer se supstituira (menja) svaki simbol poruke. Analizirane su neke od nestandardnih supstitucijskih šifri.

Ostatak rada organiziran je na sledeći način. Posle uvodnih napomena u drugom delu rada navedene su neke definicije i pojmovi, koji su potrebni za olakšano praćenje rada. Treći deo rada opisuje pojam supstitucijskih šifri. Pigpen šifre, Polybiusov kvadrat i nasumične supstitucijske šifre su opisane i analizirane u četvrtom delu. U odjeljku pet, eksperimentalni rad sa studijom slučaja objašnjen je detaljan postupak šifriranja i dešifriranja iste poruke u svim navedenim nestandardnim supstitucijskim šiframa. Urađena je komparativna analiza, navedene su prednosti i nedostaci metoda.

Danas, u doba razmene poruka globalnim računarskim i komunikacijskim mrežama, kriptografija se široko primenjuje: bez obzira da li se želi obezbediti privatnost poruka, ili se nastoji zaštititi njihova tajnost (Azizović i Maznikar, 2019). Kriptografija proučava podatke u digitalnom obliku, postupci kriptovanja i dekriptovanja matematičke su prirode, i sprovode se automatski, pomoću računara. Iz tih razloga se savremena kriptologija pretežno oslanja na računarstvo, a u velikoj meri je podržana teorijom brojeva.

2. ZNAČAJNI POJMOVI

U ovom delu navešćemo značajne definicije koje su neophodne da bi se uspešno pratio sadržaj rada (Dujella i Maretić, 2007).

Kriptologija je nauka koja se bavi izučavanjem i definisanjem metoda za zaštitu informacija (šifriranjem) i izučavanjem i pronalaženjem metoda za otkrivanje šifriranih informacija (dešifiranjem). U tu svrhu koristi znanja iz matematike, statistike i lingvistike. Rezultate kriptologije prvenstveno koriste oružane snage i diplomatska služba, a razvojem telekomunikacija i mnoge druge službe. Kriptologija obuhvata kriptografiju i kriptoanalizu.

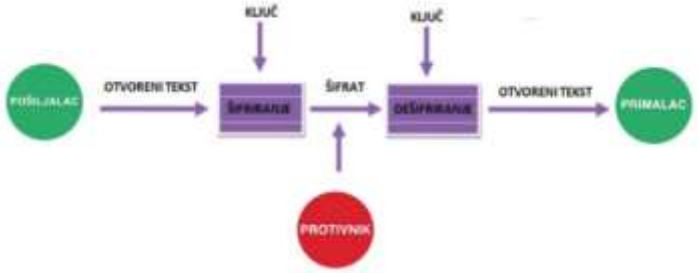
Kriptografija je naučna disciplina koja izučava metode koje omogućavaju komunikacijsku sigurnost izmedu dve osobe – pošiljalaca i primaoca poruke. Za razliku od steganografije gde se skriva da poruka postoji, kod kriptografije je presudno da ako poruka dođe u posed protivnika, on tu poruku ne može da razume. Riječ kriptografija dolazi iz grčkog jezika i znači tajno pisanje.

Kriptoanaliza ili dekriptovanje je naučna disciplina koja proučava postupke za razumevanje šifrovanih poruka bez poznavanja pravila šifrovanja i ključa pri čemu se koriste znanja iz lingvistike, matematike i statistike. Kriptoanaliza se može provesti nagađanjem ključa ili korišćenjem informacija o sistemu koji se napada. Nije nužno da je smisao kriptoanalize narušavanje privatnosti. Naprotiv, kriptografija i kriptoanaliza se nadovezuju jer pored prikupljanja informacija značaj kriptoanalize i otkrivanje grešaka i nedostataka u kriptografskim algoritmima.

Supstitucijske šifre: svaki element otvorenog teksta zamenjuje se sa nekim drugim elementom, prema unapred utvrđenoj transformaciji. U zavisnosti od broja transformacija, one mogu biti monoalfabetske i polialfabetske"

Napadom zovemo svaku usmerenu radnju kriptoanalitičara.

Slika 1: Primena kriptografskog algoritma



Izvor: Obrada autora na osnovu (Dujella i Maretić, 2007)

Na osnovu (Veinović i Adamović, 2013):

Definicija 1. Kriptosistem je uređena petorka (P, C, K, E, D) za koju vredi:

1) P je konačan skup svih mogućih osnovnih elemenata otvorenog teksta;
2) C je konačan skup svih mogućih osnovnih elemenata šifrata;
3) K je prostor ključeva, tj. konačan skup svih mogućih ključeva;
4) E je skup svih funkcija šifriranja;
5) D je skup svih funkcija dešifriranja;

Za svaki $K \in K$ postoji funkcija šifriranja $eK \in E$ i odgovarajuća funkcija dešifriranja $dK \in D$. Pritom su $eK : P \rightarrow C$ i $dK : C \rightarrow P$ funkcije sa svojstvom da je $dK(eK(x)) = x$ za svaki otvoreni tekst $x \in P$.

Iz svojstva $dK(eK(x)) = x$ slijedi kako funkcije šifriranja $eK(x)$ moraju biti injekcije. U suprotnom bi poruka mogla biti dvosmislena. Ako bi se dva različita slova otvorenog teksta $x1$ i $x2$ nekom funkcijom šifriranja šifrirala istim slovom y, tj. $eK(x1) = eK(x2) = y$, primaoc poruke neće znati treba li y dešifrirati u $x1$ ili $x2$.

Pošiljalac i primalac prvo biraju ključ $K \in K$. Pošiljalac sada šalje poruku $x=x1x2...xn$ za neki celi broj $n>0$, $xi \in P$, $0<i<n+1$. Svaki xi je šifriran.

Značaj zaštite i bezbednosti podataka je veći nego ikad. Evropska unija se odavno bavi digitalnom pismenosti i digitalnim kompetencijama, ali od 2006. su među osam najvažnijih kompetencija za život i rad uključili i digitalne kompetencije (Azizović i Maznikar, 2019). Sve kompetencije (ukupno 21) su grupisane u 5 oblasti digitalnih kompetencija: Informaciona i podatkovna pismenost, Komunikacija i Kolaboracija, Kreiranje digitalnih sadržaja, Sigurnost i Rešavanje problema. Sigurnost podataka je jedna od 5 oblasti digitalnih kompetencija i svakim danom sve više dobija na važnosti

3. SUPSTITUCIJSKE ŠIFRE

Šifre supstitucije ili zamene upoređuju se sa šifrom transpozicija. Kriptosistemi na osnovu tipa operacije koje primenjuju kod šifriranja klasifikuju se na transpozicijske i supstitucijske i kriptosisteme koji su kombinacija ova dva sistema. Transpozicijske šifre su takve gde se sadržaj otvorenog teksta permutuje (premešta). Tako na primer ako reč GRAD šifrujemo u ADGR, onda smo uradili transpoziciju.

Kod šifri supstitucije svaki element otvorenog teksta (karakter, slovo, bit, nekoliko bitova ili slova) zamenjuje nekim drugim karakterom, bitom ili slovom prema unapred utvrđenoj transformaciji. Naziv supstitucijske šifre dolazi od toga što se nešto menja, odnosno, supstituiše se svako slovo naše poruke[1].

U radu su prikazane neke od nestandardnih supstitucijskih šifri, tu spadaju monoalfabetske i polialfabetske supstitucijske šifre. Kod monoalfabetskih šifri svako slovo ili karakter ima tačno jedno supstitucijsko slovo ili karakter. To jest, ako je kod za slovo E jednak slovu L, tada u šifri slovo L uvek ima značenje slova E. Dok, kod polialfabetskog šifriranja karakter može biti šifriran sa više karaktera, ali isto tako više karaktera može biti šifrirano istim karakterom. To u stvari zavisi od pozicije u tekstu. Osim njih imamo još i monogramske i poligramske supstitucijske šifre.

Karakteristika supstitucijskih šifri je da se postupak supstitucije vrlo jednostavno pamti. Ako je ključ za dešifrovanje prost, zainteresovana strana može vrlo lako razbiti šifru i razumeti poruku.

Supstitucijske šifre susrećemo u svakodnevnom životu: tačke i crtice u Morseovoj abecedi, kod kombinacije Brailleovog pisma, komunikaciji bubnjevima afričkih plemena, znakovni jezik. To, naravno, nisu šifre, ali su primer zamene slova i reči sa simbolima" (Ibrahimpašić, 2011).

4. NESTANDARDNE SUPSTITUCIJSKE ŠIFRE

Nestandardne supstitucijjske šifre, su šifre koje ne koriste slova za supstituciju, već se koriste drugi simboli. Kod pigpen šifre slova se zamenjuju simbolima, dok kod šifrovanja Polybiusovim kvadratom slovo se šifruje sa dva broja, dok se kod nasumičnog šifriranja slovo zamenjuje proizvoljnim simbolom.

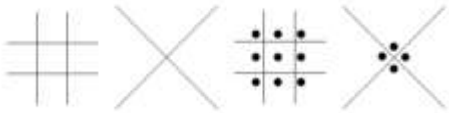
Pigpen šifra

Pigpen (*engl. svinjac)* šifra pripada je monoalfabetskim supstitucijskim šiframa u kojoj se slova supstituišu simbolima koji su prikazani kao delovi rešetke. Ova šifra dobila je ime po načinu kako se slova odvajaju linijama, baš poput svinja u svinjcu. Ova šifra još je poznata kao masonska šifra koju je koristilo masonsko društvo otprilike

[1] https://web.math.pmf.unizg.hr/~duje/kript/kriptografija.html. Pristupljeno: 24.5.2022.

početkom 18. veka. Masonsko društvo ovu je šifru pretežno koristilo kako bi se zaštitili neki od istorijskih zapisa i zapisi o obredima“(Singh, 2003). Na slici 2 su prikazani elementarni oblici pigpen šifre.

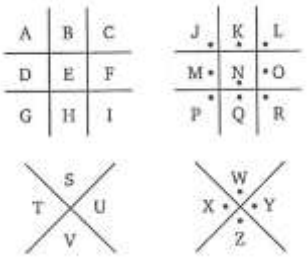
Slika 2: Elementarni oblik pigpen šifre



Izvor: Obrada autora na osnovu (Veinović i Adamović 2013)

Postupak, prvo se nacrta polje slično igri iks-oks i veliko slovo X, zatim se ponovno crtaju ista polja, stim što sada u svakom odeljku stavljamo tačku, kao što se vidi na slici 2. Onda se ispisuju abecedna slova u sva polja na crtežima. Slova se ispisuju na osnovu proizvoljnog poredka. Na slici 3 može se videti da su slova abecede napisana prema desno u svakom redu iks-oks tabele, od prvog ka poslednjem. Dok u X karakteru slova su raspoređena od vrha nalevo, onda desno i završava sa donjim.
Poruka se šifruje tako što se svako slovo suspstituiše delom crteža polja u kojem je zapisano.

Slika 3: Elementarni oblik pigpen šifre sa redosledom slova po sopstvenom izboru



Izvor: Obrada autora na osnovu (Veinović i Adamović 2013)

Polybiusov kvadrat

Ovaj kvadrat izmislio poznati grčki istoričar i naučnik Polybius (200.god pre nove ere - 118.pre nove ere). On je izmislio kvadrat radi smanjivanja broja slova u tekstu. U tabeli 1. možemo videti osnovni oblik Polybiusovog kvadrata sa engleskom azbukom. Kao što je prikazano, slova engleske azbuke zapisuj se u matricu 5 × 5. Redovi i kolone se numerišu od 1 do 5 gde svako slovo predstavlja odgovarajući par redova i kolona. (Baumslag, Fine, Kreuzer, Rosenberger, 2015).

Tabela 1: Polybiusov kvadrat sa engleskom abecedom

	1	2	3	4	5
1	*A*	*B*	*C*	*D*	*E*
2	*F*	*G*	*H*	*I/J*	*K*
3	*L*	*M*	*N*	*O*	*P*
4	*Q*	*R*	*S*	*T*	*V*
5	*V*	*W*	*X*	*Y*	*Z*

Izvor: Obrada autora

Možemo primetiti da se slova I i J nalaze u istoj ćeliji. Takođe, čest je slučaj da i slova V i W dele istu ćeliju, u zavisnosti od vrste abecede sa kojom se radi. Generalno, koje ćemo slovo primeniti, najčešće se određuje na osnovu konteksta same poruke. To jest, slova zamenjujemo ciframa redova i kolona gde je to slovo napisano. Na primer reč GRAD zapisali bismo kao 22- 42-11-14. Slova u tabeli mogu biti zapisana i sa ključnom rečju.

Nasumične supstitucijske šifre

Karakteristike šifri koje smo koristili u ovom radu su da se koristila abeceda koja je ispisana prema pravilima koja se odnosila za šifru koja se primenjivala. Najveći benefit kod takvih šifri je taj što za njihovo “razbijanje” nije neophodno nositi ključ. Ali nasumične supstitucijske šifre su šifre koje su konstruirane bez bilo kakvih pravila, tj. uz svako slovo abecede može da se postavi bilo koji karakter ili simbol.

Specifičnost takvih šifri je da ih je jako teško razbiti, tj. daleko teže od razbijanja šifri utemeljenih na prostijim sistemima. Veliki broj detektivskih priča i romana koristile su nasumične šifre kao bitne delove svojih radnji, u kojoj šifra koristi brojeve i razne simbole (Ibrahimpašić, 2011).

Tabela 2. Abeceda kodirana proizvoljnim simbolima

A= ←	J= ⇔	S= ∑
B= ↑	K= ⇔	T= ⌠
C= →	L= ⇐	U= ⏐
D= ↓	M= ⇑	V= ⌡
E= ±	N= ⇒	W= ⌠
F= ≥	O= ⇓	X= ⏐
G= ×	P= ◊	Y= ⌡
H= ∧	Q= ®	Z= ⌇
I= ∨	R= ©	

Izvor: Obrada autora

5. EKSPERIMENTALNI RAD

Primeri primene supstitucijskih šifri

U ovom delu rada čemo prikazati primere šifriranja i dešifriranja nestandardnim supstitucijskim šiframa, poruku:

PRIZREN JE LEP GRAD

Pigpen šifra

Ova šifra je poznata i kao šifra kojiu su koristili masoni. To je monoalfabetska zamenska šifra gde se slova zamenjuju karakterima koji su delovi mreže. Ukupno, dobijamo 26 razmaka koji se podudarni sa 26 slova u latinskoj abecedi. Svaki se odeljak može unikatno prepoznati ako kombinujemo oblik odsečka i da li je prisutna ili odsutna točka u njemu. Ovaj način šifriranja je relativno popularan. Zbog što komplikovanijeg razbijanja poruke, slova treba ispisivati nekim neuobičajnim rasporedom npr. za razliku od oblika prikazanog na slici 3. tj. kreirati da slova idu u različitim pravcima.

Primer 1. Šifriranje poruke pigpen supstitucijom:

Poruka se šifrira tako što se svako slovo poruke supstituiše malim crtežom odeljka u kojem je slovo napisano, tj. korišćenjem identifikatora odeljka umesto stvarnog slova. Za našu poruku, na osnovu slike 3 dobijamo[2]:

Slika 4. Šifrat dobiven pigpen šifrom

Izvor: Obrada autora

Polybiusov kvadrat

Starogrčki pisac Polybius je predložio metodu zamene svakog karaktera drugačijim dvocifrenim brojem.

Primer 2. Šifriranje poruke Polybiusovim kvadratom

Za kodiranje, potrebno je zameniti slovo sa dvocifrenim brojem gde je na prvoj poziciji broj reda a na drugoj poziciji broj kolone. Korišćenjem tabele 2. naša poruka kodirana postaje[3]:

35-42-24-55-42-15-33 24-15 31-15-35 22-42-11-14

Dešifrovanje se sprovodi tako što treba pročitati broj, prva cifra predstavlja red, dok druga sifra kolonu. Npr. 42 je četvrti red, druga kolona, u kojem je slovo R. Kod ovog šifriranja slova u tablici možemo zapisati i sa nekom ključnom reči.

[2] https://www.boxentriq.com/code-breaking, Pristupljeno: 26.5.2022.
[3] https://www.boxentriq.com/code-breaking, Pristupljeno: 26.5.2022.

Kod ovag vida šifriranja je vrlo niska komunikacijska bezbednost. U nekim slučajevima i bez korišćenja računara, šifra se lako dešifruje, naročito za duže poruke. Danas imamo veliki broj aplikacija za kriptiranje ovakvih poruka koje se koriste u zabavne svrhe.

Nasumične šifre

Nasumične šifre se konstruišu tako što ne postoje nikakva pravila ili planovi. One se mogu kreirati pridruživanjem svakom slovu neki od simbola. Za dekodiranje šifre mora se nositi ključ.

Primer 3. Šifriranje poruke nasumičnom šifrom

Na osnovu abecede koju smo kodirali proizvoljnim simbolima (tabela 2) kodiranjem naše poruke dobijamo šifru koja će izgledati vrlo tajanstveno:

Slika 5. Šifrat dobiven nasumičnom šifrom

Izvor: Obrada autora

Dobiveni simboli ne doprinose da poruka bude teža za dešifrovanje nego kod onih koji su napisani brojevima i slovima.

6. ZAKLJUČAK

Kriptografija se vekovima koristila za obezbeđivanje tajne komunikacije najčešće za diplomatske i vojne svrhe. Zamenske šifre imaju vrlo veliki značaj za kriptografiju kao nauku, sobzirom da se dugo razvijaju, razvijeni su različiti kriptosistemi, gde je svaki naredni sistem pokušavao korigovati neki nedostatak prethodnog. Ti nedostaci najčešće su se otkrivali uvek novim nastojanjima za uspešnim napadima na pojedine sisteme šifrovanja.

Danas postoji značajno interesovanje i neophodnost za konstantnim usavršavanjem i širenjem kriptografskih modela na šta ukazuje rezultat ovog istraživanja i drugih sličnih istraživanja, jer u današnje vreme kriptosistemi imaju važnu ulogu u savremenoj tehnologiji koja se koristi za komunikaciju, za šta je neophodna bezbednost i privatnost.

Ciljevi rada su dokazani, kriptosistemi koje smo obradili u radu, kao i drugi važni sistemi, predstavljaju osnovnu bazu za razvoj savremenih bezbedonosnih računarskih sistema koji se danas koriste u svim oblastima ljudskog života. Sa razvojem novih tehnologija za prijenos informacija i poruka javlja se i neophodnost za njihovu zaštitu.

Što se tiće novih istraživanja, posle ove osnovne analize, planiramo detaljniju analizu ostalih polialfabetskih supstitucijskih šifri. Kao i unapređenje implementacije predloženih rešenja u oblasti supstitucijskih šifri u tim modelima.

U vreme kada se skoro svakog dana dešavaju skandali oko neovlašćenog pristupa i korišćenja informacija neophodnost za njihovom bezbednošću je veća nego ikad u istoriji čovečanstva. Poneke od najboljih metoda sigurnosti informacija i podataka se zapravo nalaze u sistemu šifriranja.

LITERATURA

Azizović, E., & Maznikar, B. (2019). *Digital competences of public notaries*, Knowledge in practice -International Journal, Vol. 35 No. 5.

Baumslag, G., Fine, B., Kreuzer, M., & Rosenberger, G. (2015). *A Course in Mat- hematical Cryptography*, De Gruyter, Boston.

Dujella, A. (2019). *Teorija brojeva*, Školska knjiga, Zagreb.

Dujella, A., & Maretić, M. (2007). *Kriptografija*, Element, Zagreb.

Ibrahimpašić, B. (2011). *Kriptografija kroz primjere*, Pedagoški fakultet Bihač.

Kahn, D. (1967). *The Code-Breakers: The Story of Secret Writing*, The Macmillan Company, New York.

Matić, I. (2015). *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište u Osijeku.

Singh, S. (2003). *Šifre : Kratka povijest kriptografije*, Mozaik knjiga, Zagreb.

Veinović, M., & Adamović, S. (2013). *Kriptologija 1*, Univerzitet Singidunum, Beograd.

https://web.math.pmf.unizg.hr/~duje/kript/kriptografija.html, Pristupljeno: 24.5.2022.

https://www.boxentriq.com/code-breaking, Pristupljeno: 26.5.2022.