

Primjene linearne algebre u kriptanalizi

Brežnjak, Darko

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:200:889826>

Rights / Prava: [In copyright](#) / [Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-04-25**

Repository / Repozitorij:

[Faculty of Electrical Engineering, Computer Science and Information Technology Osijek](#)



SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I
INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

PRIMJENE LINEARNE ALGEBRE U KRIPTOANALIZI

Diplomski rad

Darko Brežnjak

Osijek, 2016. godina

**FERIT**FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK****Obrazac D1: Obrazac za imenovanje Povjerenstva za obranu diplomskog rada**

Osijek, 26.09.2016.

Odboru za završne i diplomske ispite**Imenovanje Povjerenstva za obranu diplomskog rada**

Ime i prezime studenta:	Darko Brežnjak
Studij, smjer:	Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika
Mat. br. studenta, godina upisa:	D-865, 03.10.2014.
OIB studenta:	54843501908
Mentor:	Doc.dr.sc. Tomislav Rudec
Sumentor:	Doc.dr.sc. Alfonzo Baumgartner
Predsjednik Povjerenstva:	Doc.dr.sc. Anita Katić
Član Povjerenstva:	Doc.dr.sc. Alfonzo Baumgartner
Naslov diplomskog rada:	Primjene linearne algebre u kriptanalizi
Znanstvena grana rada:	Obradba informacija (zn. polje računarstvo)
Zadatak diplomskog rada:	Tema je zauzeta - Darko Brežnjak
Prijedlog ocjene pismenog dijela ispita (diplomskog rada):	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 3 Postignuti rezultati u odnosu na složenost zadatka: 3 Jasnoća pismenog izražavanja: 3 Razina samostalnosti: 3
Datum prijedloga ocjene mentora:	26.09.2016.
Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

**FERIT**FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK****IZJAVA O ORIGINALNOSTI RADA****Osijek, 02.10.2016.****Ime i prezime studenta:**

Darko Brežnjak

Studij:

Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika

Mat. br. studenta, godina upisa:

D-865, 03.10.2014.

Ephorus podudaranje [%]:

2 %

Ovom izjavom izjavljujem da je rad pod nazivom: **Primjene linearne algebre u kriptanalizi**

izrađen pod vodstvom mentora Doc.dr.sc. Tomislav Rudec

i sumentora Doc.dr.sc. Alfonzo Baumgartner

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.

Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

SADRŽAJ	1
1. UVOD	2
2. LINEARNA ALGEBRA.....	3
2.1 Matrice	3
2.1.1 Algebra matrica	3
2.1.2 Determinante	7
2.1.3 Inverz matrice.....	8
2.2 Vektorski prostor i potprostor	9
2.4 Rastavi matrica i algoritmi redukcije	10
2.4.1 Gaussova metoda eliminacije.....	10
2.4.2 Gram-Schmidtov postupak.....	12
2.4.3 Rastav na singularne vrijednosti	12
2.4.4 Gaussova redukcija rešetke dimenzije 2	13
3. KRIPTOANALIZA.....	14
3.1 Osnovni pojmovi.....	14
3.2 Kriptoanaliza monoalfabetskih supstitucijskih šifri.....	15
3.2.1 Matrica frekvencije bigrama	15
3.2.1 Primjena rastava na singularne vrijednosti.....	17
3.3 Kriptoanaliza Hillove šifre	20
3.4 Kriptoanaliza kongurentnih kriptosustava s javnim ključem	23
3.4.1 Korištenje kongurentnih kriptosustava s javnim ključem	24
3.4.2 Kriptoanaliza kongurentnih kriptosustava s javnim ključem	25
4. Zaključak	27
LITERATURA.....	28

1. UVOD

Linearna algebra te matematički alati koji su razvijeni njenom primjenom u prirodnim i tehničkim znanostima našli su svoju primjenu i u kriptologiji. Razlog tome nije samo njihova linearna priroda nego i jednostavnost implementacije istih alata te algoritama i funkcija na računalu što je izuzetno važno u suvremenim informatiziranim kriptografskim sustavima. [1],[2]

Zadatak ovog diplomskog rada je istražiti ulogu linearne algebre u kriptologiji te navesti osnove ove discipline. Kroz predstojeća poglavlja pokušat će se kvalitetno obraditi neke osnovne primjene alata iz linearne algebre u grani kriptologije koja se, između ostalog, bavi analizom kriptografskih sustava – kriptanaliza.

U drugom poglavlju proveden je kratak uvod u linearnu algebru. Razložena su osnovna svojstva matrica i operacija s matricama, obrađeni neki osnovni pojmovi vezani za vektore i vektorske prostore, a koji su bitni za obradu glavne ideje ovoga rada. Dodatno su u istom poglavlju navedeni i opisani neki od korisnijih algoritama u analizi vektora i matrica.

U trećem se poglavlju uvode osnovne ideje te pojmovi kriptologije i kriptanalize, ali i razrađuju konkretni primjeri kriptanalitičkih napada baziranih na primjenama linearne algebre.

2. LINEARNA ALGEBRA

Osnovni zadatak linearne algebre je traženje rješenja sustava linearnih jednačbi odnosno $m \times n$ linearnog sustava gdje m označava broj jednačbi, a n broj nepoznanica sadržanih u jednačbama sustava. *Linearna jednačba* sa nepoznaticama $x_1, \dots, x_n$ je jednačba koja se može zapisati u obliku

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b, \quad (2-1)$$

gdje su b i koeficijenti $a_1, \dots, a_n$ realni ili kompleksni brojevi. *Sustav $m \times n$ linearnih jednačbi* se tada generalno može zapisati kao:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m. \end{aligned} \quad (2-2)$$

U linearnoj algebri se sustav iz (2-2) kompaktnije zapisuje u *matričnom obliku* kao umnožak

$$A\mathbf{x} = \mathbf{b}, \quad (2-3)$$

gdje je A matrica koeficijenata a_{mn} , $\mathbf{x}$ vektor čije su komponente nepoznanice x_n te $\mathbf{b}$ također vektor, ali čiji su koeficijenti konstante s desne strane jednakosti u sustava (2-2). Uzimajući u obzir (2-2) i (2-3) dobiva se zapis

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ & & \ddots & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}. \quad (2-4)$$

2.1 Matrice

2.1.1 Algebra matrica

Operacija zbrajanja matrica definirana je za matrice istih dimenzija, odnosno **istog tipa**. Skup svih matrica istog tipa $m \times n$ označava se sa $\mathbf{M}_{mn}$. Operacija se provodi zbrajanjem „član po član“, to jest međusobno se zbroje elementi matrica s istim indeksom pa vrijedi

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} + \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{bmatrix} = \begin{bmatrix} a_{11} + b_{11} & \cdots & a_{1n} + b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & \cdots & a_{mn} + b_{mn} \end{bmatrix}, \quad (2-5)$$

odnosno

$$A + B = C. \quad (2-6)$$

Rezultat zbrajanja je opet matrica istog tipa kao i sumandne matrice. Za operaciju zbrajanja $m \times n$ matrica A, B i C definirana su sljedeća algebarska svojstva:

- (1) Zatvorenost: $A_{m \times n} + B_{m \times n}$ daje ponovo matricu dimenzija $m \times n$,
- (2) Asocijativnost: $(A + B) + C = A + (B + C)$,
- (3) Komutativnost: $A + B = B + A$,
- (4) Neutralni element: $m \times n$ matrica $\mathbf{0}$ (tzv. *nul-matrica*), čiji su svi elementi jednaki nuli, ima svojstvo da je $A + \mathbf{0} = A$,
- (5) Inverzni element: $m \times n$ matrica $(-A)$ ima svojstvo da je $A + (-A) = \mathbf{0}$.

Množenje matrice $A \in \mathbf{M}_{mn}$ skalarom $\lambda \in \mathbb{R}$ vrši se na način da skalar množi svaki element matrice pa je

$$\lambda A = \lambda \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} = \begin{bmatrix} \lambda a_{11} & \cdots & \lambda a_{1n} \\ \vdots & \ddots & \vdots \\ \lambda a_{m1} & \cdots & \lambda a_{mn} \end{bmatrix}. \quad (2-7)$$

Za množenja skalare λ i γ i matrica A i B vrijede sljedeća svojstva:

- (1) Zatvorenost: $\lambda A_{m \times n}$ daje ponovo matricu dimenzija $m \times n$,
- (2) Asocijativnost: $(\lambda\gamma)A = \lambda(\gamma A)$,
- (3) Distributivnost: $\lambda(A + B) = \lambda A + \lambda B$ - skalarno množenje je distributivno prema zbrajanju matrica,
- (4) Distributivnost: $(\lambda + \gamma)A = \lambda A + \gamma A$ - skalarno množenje je distributivno prema skalarom množenju,
- (5) Jedinični element: $1A = A$.

Matrica dimenzije $m \times n$ množi se vektorom dimenzije n po principu skalarnog umnoška vektora pa vrijedi:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}, \quad (2-8)$$

odnosno

$$A\mathbf{x} = \mathbf{b}. \quad (2-9)$$

Umnožak matrice A i vektora $\mathbf{x}$, s njezine desne strane, može se interpretirati i kao **linearna kombinacija** stupaca od A i elemenata od $\mathbf{x}$ što daje:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = x_1 \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} + x_2 \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} + \cdots + x_n \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}. \quad (2-10)$$

Stupci ili retci neke matrice nazivaju se još redom i vektor-stupci ili vektor-retci.

Množenje matrice A dimenzija $m \times n$ s matricom B dimenzija $n \times p$ daje kao rezultat matricu C dimenzija $m \times p$ kao što je to vidljivo iz formule (2-10). Da bi postojao umnožak matrica, one moraju biti **ulančane**. Za dvije se matrice, čiji se umnožak želi pronaći, kaže se da su ulančane kada je broj stupaca matrice s lijeva jednak broju redaka matrice s desna znaka operacije množenja. Znak operacije množenja je obično praznina ili ponekad točka „ $\cdot$ “.

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1p} \\ b_{21} & b_{22} & \cdots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{np} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1p} \\ c_{21} & c_{22} & \cdots & c_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mp} \end{bmatrix}. \quad (2-11)$$

Svaki element matrice C dobiven je skalarnim umnoškom x -tog vektor-retka matrice A i y -tog vektor-stupca matrice B . Prema tome element c_{xy} je jednak umnošku

$$[a_{x1} \ a_{x2} \ \cdots \ a_{xn}] \begin{bmatrix} b_{1y} \\ b_{2y} \\ \vdots \\ b_{ny} \end{bmatrix} = a_{x1}b_{1y} + a_{x2}b_{2y} + \cdots + a_{xn}b_{ny} = c_{xy}$$

te se na primjer za $x=2$ i $y=1$ dobiva element c_{21} (element na sjecištu 2. retka i 1. stupca). Primjenom (2-10), množenje matrice A matricom B ekvivalentno je linearnoj kombinaciji n -tog vektor-stupaca matrice A i elemenata pripadnog y -tog vektor-stupca matrice B .

$$A B = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1p} \\ b_{21} & b_{22} & \cdots & b_{2p} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{np} \end{bmatrix} = C = \left[\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} \right],$$

$$b_{11} \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} + b_{21} \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} + \cdots + b_{n1} \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix} = \begin{bmatrix} c_{11} \\ c_{21} \\ \vdots \\ c_{m1} \end{bmatrix} = \mathbf{c}_1,$$

$$b_{12} \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} + b_{22} \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} + \cdots + b_{n2} \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix} = \begin{bmatrix} c_{12} \\ c_{22} \\ \vdots \\ c_{m2} \end{bmatrix} = \mathbf{c}_2,$$

$$\vdots$$

$$b_{1p} \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} + b_{2p} \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} + \cdots + b_{np} \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix} = \begin{bmatrix} c_{1n} \\ c_{2n} \\ \vdots \\ c_{mn} \end{bmatrix} = \mathbf{c}_n.$$

Svaki od vektora $\mathbf{c}_n$, dobivenog linearnom kombinacijom $A\mathbf{b}$, predstavlja jedan vektor-stupac rezultirajuće matrice C .

Još jedna važna operacija nad matricama naziva se **transponiranje**. Transponiranjem matrice $A_{m \times n}$ dobiva se matrica $A^T = A_{n \times m}$ čiji su retci n zapravo stupci matrice A . Samim time stupci m od A^T su retci od A . Jednostavnije rečeno, transponiranjem se vrši zamjena redaka i stupaca neke matrice: ako je $A = [a_{ij}]$, tada je $[A^T]_{ij} = a_{ji}$. Na primjer,

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{bmatrix}^T = \begin{bmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \end{bmatrix} \quad (2-12)$$

i ovaj postupak vrijedi za matrice bilo kojih dimenzija.

Matrično množenje posjeduje neka očekivana dobra svojstva:

- (1) Asocijativnost: $(AB)C = A(BC)$,
- (2) Distributivnost: $(A + B)C = AC + BC$,
- (3) Jedinичna matrica: $AI = IA = A$,
- (4) Inverzni element: $(AB)^T = B^T A^T$.

Važno je naglasiti i da za svaku matricu A vrijedi da je $(A^T)^T = A$ te da za umnožak vektor-retka i vektor-stupca vrijedi $\mathbf{a}^T \mathbf{b} = \mathbf{b}^T \mathbf{a}$.

2.1.2 Determinante

Determinanta matrice „ $\det$ “ je funkcija koja svakoj kvadratnoj matrici pridružuje skalar. Za slučaj da je matrica A realna, vrijednost funkcije

$$\det : A \rightarrow \mathbb{R}, \quad (2-13)$$

je realan broj. Osim oznake $\det$, determinanta se često označava vertikalnim crtama $\begin{vmatrix} & \end{vmatrix}$ oko oznake za matricu (npr. $|A|$) ili elemenata matrice (kao u izrazu 2-14). Za kvadratnu 2×2 matricu determinanta se definira na sljedeći način:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} := a_{11}a_{22} - a_{12}a_{21}. \quad (2-14)$$

Determinanta kvadratnih matrica dimenzija 3×3 definira se po sličnom principu i vrijedi

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}. \quad (2-15)$$

Potonji se princip izračunavanja determinante naziva **Laplaceov razvoj determinante** i često se primjenjuje kod matrica trećeg ili višeg reda. Ovdje se determinanta matrice definira razvojem po nekom retku, odnosno stupcu matrice. Determinanta matrice reda n definira se razvojem po i -tom retku preko

$$\det A = \sum_{j=1}^n a_{ij} A_{ij} = \sum_{j=1}^n (-1)^{i+j} a_{ij} M_{ij}, \quad (2-16)$$

ili pak razvojem po j -tom stupcu preko

$$\det A = \sum_{i=1}^n a_{ij} A_{ij} = \sum_{i=1}^n (-1)^{i+j} a_{ij} M_{ij}. \quad (2-17)$$

Oznaka a_{ij} određuje elemente prvog retka/stupca, a M_{ij} označava pripadajuće **minore** (minora je naziv za determinantu matrice dobivenu brisanjem i -tog retka i j -tog stupca).

Nadalje, korisno je navesti i nekoliko najvažnijih svojstava determinanti. Svojstva će biti iskazana za retke determinanti, ali tvrdnje vrijede i ako se riječ redak zamijeni s riječi stupac.

(1) Ako matrica A ima reda sastavljen od samih nula, onda je $\det A = 0$,

- (2) Determinanta trokutaste matrice jednaka je umnošku elemenata na dijagonali,
- (3) Ako matrica A ima dva jednaka retka, onda je $\det A = 0$,
- (4) Transponiranjem matrice vrijednost determinante se ne mijenja,
- (5) Determinanta se množi skalarom tako da se jedan (bilo koji) njen redak množi tim skalarom,
- (6) Rastave li se svi elementi nekog retka matrice na zbroj dvaju elemenata, onda je determinanta jednaka zbroju dviju odgovarajućih determinanti,
- (7) Ako se zamijene dva retka matrice determinanta mijenja predznak,
- (8) Ako nekom retku matrice dodamo neki drugi redak pomnožen skalarom vrijednost determinante neće se promijeniti,
- (9) Determinanta produkta dviju matrica jednaka je produktu determinanti (*Binet-Cauchyjeve teoreme*).

2.1.3 Inverz matrice

Za danu kvadratnu matricu $A_{n \times n}$, matrica $B_{n \times n}$ koja zadovoljava uvjet:

$$AB = I_n \text{ i } BA = I_n, \quad (2-18)$$

naziva se **inverz matrice** A i označava se sa $B = A^{-1}$. Matrice za koje postoji inverz nazivaju se *invertibilne*, *regularne* ili *nesingularne*, odnosno za slučaj da ne postoji inverz tada se takva matrica naziva *singularnom matricom*. Važno je ponoviti, ali drugim riječima, da je inverz matrice definiran samo za kvadratne matrice.

U slučaju da inverz dane matrice postoji tada je on jedinstven. Kod dokazivanja ove tvrdnje pretpostavi se da postoje dva nejednaka inverza X_1 i X_2 neke nesingularne matrice. Tada vrijedi

$$X_1 = X_1 I = X_1 (A X_2) = (X_1 A) X_2 = I X_2 = X_2$$

i prema tome postoji samo jedan, jedinstveni, inverz. Primjenom Binet-Cauchyjevog teorema (svojstvo (9) iz točke 2.3) slijedi

$$\det(A^{-1}A) = \det(A^{-1}) \det(A) = \det I = 1,$$

što ukazuje da za regularnu matricu mora biti $\det(A) \neq 0$. Eksplicitni zapis inverzne matrice može se predložiti zapisom

$$A^{-1} = \frac{1}{\det A} \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}^T. \quad (2-19)$$

2.2 Vektorski prostor i potprostor

Skup svih matrica M_{mn} uz operacije zbrajanja matrica i množenja skalarima i matrice čini **vektorski prostor**.

Definicija 2.2.1 Neka je V neprazan skup na kojem su zadane binarna operacija zbrajanja $+: V \times V \rightarrow V$ i operacija množenja skalarima iz polja $\mathbb{H}$, $\cdot: \mathbb{H} \times V \rightarrow V$. Kaže se da je uređena trojka $(V, +, \cdot)$ vektorski prostor nad poljem $\mathbb{H}$ ako vrijedi:

- (1) $a + (b + c) = (a + b) + c, \forall a, b, c \in V$;
- (2) postoji $0 \in V$ sa svojstvom $a + 0 = 0 + a = a, \forall a \in V$;
- (3) za svaki $a \in V$ postoji $-a \in V$ tako da je $a + (-a) = -a + a = 0$;
- (4) $a + b = b + a, \forall a, b \in V$;
- (5) $\alpha(\beta a) = (\alpha\beta)a, \forall \alpha, \beta \in \mathbb{H}, \forall a \in V$;
- (6) $(\alpha + \beta)a = \alpha a + \beta a, \forall \alpha, \beta \in \mathbb{H}, \forall a \in V$;
- (7) $\alpha(a + b) = \alpha a + \alpha b, \forall \alpha \in \mathbb{H}, \forall a, b \in V$;
- (8) $1 \cdot a = a, \forall a \in V. \quad [23]$

Ako se govori o vektorima prostora $\mathbb{R}^n$, odnosno o dvodimenzionalnom, trodimenzionalnom ili općenito n -dimenzionalnom prostoru vektora, kaže se da je to vektorski prostor *nad poljem* realnih brojeva $\mathbb{R}$. Prostor $\mathbb{R}^n$ se sastoji od *svih vektor stupaca s n komponenti*, a komponente su realni brojevi. Umjesto polja $\mathbb{R}$ može se koristiti i drugo polje skalarima, na primjer polje kompleksnih brojeva.

Vektorski se prostori mogu definirati iz podskupova nekih drugih vektorskih prostora. Tako dobiveni prostori nazivaju se *potprostori*. Bitno je napomenuti kako će sva svojstva vektorskog (nad)prostora, kao što su zatvorenost nad operacijama zbrajanja i množenja sa skalarom, vrijediti i za potprostor dobiven iz njega.

Teorem 2.2.1 Neka je X vektorski prostor. $Z \subset X$ je potprostor ako i samo ako vrijedi:

- (1) $(\forall x, y \in Z)(\forall \alpha, \beta \in \mathbb{R}) \quad \alpha x + \beta y \in Z.$

Činjenica da je Z podskup vektorskog prostora dozvoljava da se ne provjeravaju valjanosti svojstava (1), (2), (5), (6), (7) i (8), iz Definicije 2.2.1, u prostoru Z jer vrijede u većem vektorskom prostoru X .

2.4 Rastavi matrica i algoritmi redukcije

2.4.1 Gaussova metoda eliminacije

Rješenje sustava (2-2) je svaka n -torka $(x_1, \dots, x_n)$ koja uvrštena identički zadovoljava sve jednadžbe sustava. Sustav može imati jedinstveno rješenje, može biti bez ijednog rješenja, ali može imati i beskonačno mnogo rješenja.

Gaussova se metoda sastoji u tome da se sustav (2-2) *elementarnim transformacijama* svede na ekvivalentan, iz kojeg se tada može lakše odrediti njegovo rješenje. Tri pravila za dobivanje ekvivalentnog sustava svode se na specijalne operacije nad retcima matrice. To su

- (1) zamjena dvaju redaka,
- (2) množenje nekog retka skalarom različitim od nule,
- (3) dodavanje retka pomnoženog skalarom drugom retku.

Ekvivalentan sustav koji se traži kod Gaussove metode je tzv. *gornja trokutasta matrica*. U takvoj su matrici svi elementi ispod glavne dijagonale jednaki nuli. Specijalne operacije (1), (2) i (3) nad retcima matrice efikasno se provode *elementarnim matricama*.

Sustavno se rješavanje sustava najlakše može prikazati na konkretnom primjeru. Neka je zadan sljedeći 3×3 sustav:

$$x + 2y + z = 2$$

$$3x + 8y + z = 12$$

$$4y + z = 2.$$

I takav se sustav može zapisati u matičnom obliku te se dobiva sustav $Ax = b$

$$\begin{bmatrix} 1 & 2 & 1 \\ 3 & 8 & 1 \\ 0 & 4 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2 \\ 12 \\ 2 \end{bmatrix}.$$

Iz matrice se koeficijenta, matrice A , redom biraju elementi po glavnoj dijagonali (eliminacijski elementi ili pivoti) kojima se tada uz pomoć operacija množenja i oduzimanja eliminiraju svi nenul elementi ispod tog pivotnog elementa. Algoritam za konkretan slučaj je sljedeći:

$$\begin{array}{ccc}
\begin{bmatrix} \boxed{1} & 2 & 1 \\ 3 & 8 & 1 \\ 0 & 4 & 1 \end{bmatrix} & \xrightarrow{(2. \text{ redak}) - 3(1. \text{ redak})} & \begin{bmatrix} 1 & 2 & 1 \\ 0 & 2 & -2 \\ 0 & 4 & 1 \end{bmatrix}, \\
\begin{bmatrix} 1 & 2 & 1 \\ 0 & \boxed{2} & -2 \\ 0 & 4 & 1 \end{bmatrix} & \xrightarrow{(3. \text{ redak}) - 2(2. \text{ redak})} & \begin{bmatrix} 1 & 2 & 1 \\ 0 & 2 & -2 \\ 0 & 0 & 5 \end{bmatrix}.
\end{array}$$

Ovime je dobiven traženi ekvivalentni sustav U s nul-elementima ispod glavne dijagonale. U prvom se koraku prvi član u drugom retku ($a_{21} = 3$) eliminirao pomoću pivota, označenog crvenom bojom, koji je prvi član prvog retka ($a_{11} = 1$). Ovaj korak, proveden operacijama s matricama, postavljen je na sljedeći način:

$$E_{21}A = U_{21},$$

$$\begin{bmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 \\ 3 & 8 & 1 \\ 0 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 2 & -2 \\ 0 & 4 & 1 \end{bmatrix}.$$

Za sljedeći korak, u kojem se rješava element $a_{32} = 4$ pomoću pivota $a_{22} = 2$, vrijedi:

$$E_{32}U_{21} = U_{32} = U,$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 2 & -2 \\ 0 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 2 & -2 \\ 0 & 0 & 5 \end{bmatrix}.$$

Ako se svi koraci prikažu ako množenje u jednom redu tada se matrica A istim redoslijedom množi s lijeva eliminacijskim matricama:

$$E_{32}(E_{21}A) = U,$$

te primjenom svojstva asocijativnosti kod množenja matrica dobiva se matrica E koja u sebi sadržava sve provedene korake, odnosno

$$E_{32}(E_{21}A) = (E_{32}E_{21})A = EA = U.$$

Primijenjeno na obrađivani primjer dobiva se

$$\begin{array}{ccccccc}
\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 2 & 1 \\ 3 & 8 & 1 \\ 0 & 4 & 1 \end{bmatrix} & = & \begin{bmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ 6 & -2 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 2 & 1 \\ 3 & 8 & 1 \\ 0 & 4 & 1 \end{bmatrix} & = & \begin{bmatrix} 1 & 2 & 1 \\ 0 & 2 & -2 \\ 0 & 0 & 5 \end{bmatrix} \\
E_{32} & E_{21} & A & & E & A & U
\end{array}$$

2.4.2 Gram-Schmidtov postupak

U ortogonalnoj bazi, svaki je pojedinačni vektor okomit na preostale vektore baze kao npr. neki vektori koji leže na osima Kartezijevog koordinatnog sustava. Dodatno se takvi vektori mogu napraviti jediničnim tako da se komponente vektora podijele s njegovim modulom. Ako se postupak provede za sve vektore baze dobiva se **ortonormalna baza**.

Vektori $q_1, \dots, q_n$ su *ortonormalni* ako

$$q_i^T q_j = [0].$$

Neka je zadan skup linearno nezavisnih vektora

$$\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n \in \mathbb{R}^m$$

pri čemu evidentno mora biti $m \geq n$. Gram-Schmidtovim postupkom se tada konstruira ortonormirani skup vektora

$$\mathbf{q}_1, \mathbf{q}_2, \dots, \mathbf{q}_n \in \mathbb{R}^m$$

koji razapinju isti potprostor u $\mathbb{R}^m$. Postupak je sljedeći:

$$\begin{aligned} \mathbf{q}_1 &= \frac{\mathbf{a}_1}{\|\mathbf{a}_1\|}, \\ \mathbf{q}_2 &= \frac{\overline{\mathbf{a}}_2}{\|\overline{\mathbf{a}}_2\|}, \quad \overline{\mathbf{a}}_2 = \mathbf{a}_2 - (\mathbf{q}_1 \cdot \mathbf{a}_2)\mathbf{q}_1, \\ \mathbf{q}_3 &= \frac{\overline{\mathbf{a}}_3}{\|\overline{\mathbf{a}}_3\|}, \quad \overline{\mathbf{a}}_3 = \mathbf{a}_3 - (\mathbf{q}_1 \cdot \mathbf{a}_3)\mathbf{q}_1 - (\mathbf{q}_2 \cdot \mathbf{a}_3)\mathbf{q}_2, \\ &\vdots \\ \mathbf{q}_n &= \frac{\overline{\mathbf{a}}_n}{\|\overline{\mathbf{a}}_n\|}, \quad \overline{\mathbf{a}}_n = \mathbf{a}_n - \sum_{i=1}^{n-1} (\mathbf{q}_i \cdot \mathbf{a}_n)\mathbf{q}_i. \end{aligned}$$

Algoritam počinje tako da se normira jedan od vektora. U i -tom se koraku od vektora $\mathbf{a}_i$ oduzima njegova projekcija na prvih $i - 1$ vektora: $\mathbf{q}_1, \dots, \mathbf{q}_{i-1}$. Time vektor $\mathbf{q}_i$ postaje ortogonalan na sve preostale vektore.

2.4.3 Rastav na singularne vrijednosti

Teorem 2.4.2.1 *Neka je A proizvoljna matrica tipa $m \times n$, uz $m \geq n$. A se može rastaviti kao*

$$A = \hat{U} \begin{bmatrix} \Sigma \\ 0 \end{bmatrix} V^* = \hat{U} \Sigma V^*, \quad (2-20)$$

gdje je:

- $\Sigma = \text{diag}(\sigma_1, \dots, \sigma_n)$ dijagonalna matrica uz $\sigma_1 \geq \dots \geq \sigma_n \geq 0$,
- $\hat{U} = [U, U_0]$ unitarna matrica reda m ,
- V unitarna matrica reda n .

Stupci matrice $\hat{U}$ nazivaju se *lijevi singularni vektori*, stupci matrice V *desni singularni vektori* dok se dijagonalni elementi matrice Σ nazivaju *singularnim vrijednostima*.

2.4.4 Gaussova redukcija rešetke dimenzije 2

Gaussova redukcija rešetke je algoritam za pronalaženje optimalne baze dvodimenzionalne mrežaste strukture – rešetke. Osnovna je ideja višestruko oduzimanje višekratnika jednog vektora baze od drugog vektora i tako sve do trenutka kada daljnje smanjenje vektora baze nije moguće.

Uzme li se da je $L \subset \mathbb{R}^2$ neka dvodimenzionalna rešetkasta struktura čije bazne vektore označimo s $\mathbf{v}_1$ i $\mathbf{v}_2$ tako da vrijedi da je $\|\mathbf{v}_1\| < \|\mathbf{v}_2\|$. Algoritam sada nalaže, dok god je to moguće, reduciranje vektora baze $\mathbf{v}_2$ za višekratnike drugog vektora baze, $\mathbf{v}_1$. Za slučaj da je dozvoljeno oduzimanje proizvoljnog višekratnika $\mathbf{v}_1$, tada se vektor $\mathbf{v}_2$ zamjenjuje vektorom

$$\mathbf{v}_2^* = \mathbf{v}_2 - \frac{\mathbf{v}_1 \cdot \mathbf{v}_2}{\|\mathbf{v}_1\|^2} \mathbf{v}_1$$

koji je okomit na vektor $\mathbf{v}_1$. Postupak zapravo daje novi vektor $\mathbf{v}_2^*$ koji je projekcija vektora $\mathbf{v}_2$ na pravac (ili na ravninu u općenitom slučaju) okomit s $\mathbf{v}_1$.

Za slučaj da je rešetka L sačinjena od samo pozitivnih cijelobrojnih parova, vektor $\mathbf{v}_2^*$ ne mora nužno biti unutar rešetke. U praksi se dozvoljava oduzimanje samo cijelobrojnih višekratnika $\mathbf{v}_2$ od vektora $\mathbf{v}_2$. Stoga se vektor $\mathbf{v}_2$ zamjenjuje vektorom

$$\mathbf{v}_2 - m\mathbf{v}_1 \quad \text{za} \quad m = \left\lfloor \frac{\mathbf{v}_1 \cdot \mathbf{v}_2}{\|\mathbf{v}_1\|^2} \right\rfloor,$$

gdje oznaka $\lfloor x \rfloor$ određuje zaokruživanje dobivenog realnog rješenja na najbliži cijeli broj. Ako je primjenom algoritma vektor $\mathbf{v}_2$ i dalje veći, algoritam staje. Inače, izvrši se zamjena $\mathbf{v}_1$ i $\mathbf{v}_2$ te se cijeli proces ponovi.

3. KRIPTOANALIZA

Poznato je da ljudi koriste kriptografiju već gotovo 4 tisućljeća (Egipat 1900. godina p.n.e., Sparta 650. godina p.n.e. itd.) kako bi bili sigurni da prenošena poruka ne bi: bila čitljiva, imala smisla ili bi nosila krive informacije onoj osobi kojoj nije namijenjena. Osnovna je zadaća kriptanalitičara krađa informacija koje razmjenjuju pošiljalatelj i primalac preko nesigurnog komunikacijskog kanala.

3.1 Osnovni pojmovi

Svima je dobro poznato kako ljudi svakodnevno komuniciraju pomoću opće poznatih i dogovorenih niza simbola ili glasova, standard jezika i pisma, koji općenito nije isti za sva geografska područja. Pretpostavlja se da govornik (pošiljalatelj) i sugovornik (primatelj) imaju unaprijed dogovoren standard poruka kojima će komunicirati. U kriptografiji se takav oblik poruka naziva otvoreni tekst. Prema tome *otvoreni tekst* je naziv za izvorni tekst koji pošiljalatelj želi poslati primatelju, a da na njega nije primjenio šifriranje. Ako pošiljalatelj želi sakriti informaciju sadržanu u poruci, primjenom postupka šifriranja dobiti će *šifrat* (njem. *Das Chifftrat*) - označava transformirani otvoreni tekst (rezultat je šifriranja primjenom dogovorenog algoritma – funkcija, znakova, ključa itd.). *Šifriranje* ili *kriptiranje* označava niz točno određenih koraka (npr. funkcije supstitucije, transpozicije, operacija nad matricama) kojom se otvoreni tekst transformira u šifrirani tekst – šifrat. *Dešifriranje* ili *dekriptiranje* je pak obrnuti (inverzni) proces od šifriranja koji šifrirani tekst transformira natrag u otvoreni tekst. Postoji još jedan pojam usko vezan sa šifriranjem, a to je *Šifra* (engl. *Cipher*) koja označava algoritam kojom se obavlja kriptiranje i dekriptiranje.

Definicja 3.1.1 *Kriptosustav je uređena petorka $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ gdje je: $\mathcal{P}$ skup svih otvorenih tekstova, $\mathcal{C}$ konačan skup svih šifrata, $\mathcal{K}$ konačan skup svih mogućih ključeva, $\mathcal{E}$ skup svih funkcija šifriranja i $\mathcal{D}$ skup svih funkcija dešifriranja. Za svaki $k \in \mathcal{K}$ postoji $e_k \in \mathcal{E}$ i odgovarajući $d_k \in \mathcal{D}$. Pritom su $e_k: \mathcal{P} \rightarrow \mathcal{C}$ i $d_k: \mathcal{C} \rightarrow \mathcal{P}$ funkcije sa svojstvom da je $d_k(e_k(x)) = x$ za svaki $x \in \mathcal{P}$. [8]*

Nakon što su navedeni neki osnovni pojmovi, kriptanalizu je moguće točnije definirati kao granu kriptologije koja se bavi analizom šifri, šifrata i kriptosustava.

3.2 Kriptoanaliza monoalfabetskih supstitucijskih šifri

Supstitucijske šifre su vjerojatno najčešći i najjednostavniji oblik šifri uopće. Često se spominju i pod nazivom „kriptogrami“. Ideja iza monoalfabetskih supstitucijskih šifri je jednostavna: zamjena jednog simbola otvorenog teksta (npr. simbola engleskog alfabeta) s drugim simbolom istog ili drugog alfabeta daje šifrat odnosno šifrirani tekst.

Definicija 3.2.1 *Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. $\mathcal{K}$ se sastoji od svih mogućih permutacija 26 simbola: $0, 1, \dots, 25$. Za svaku permutaciju $\pi \in \mathcal{K}$ definira se*

$$e_{\pi}(x) = \pi(x) \quad (3-1)$$

i

$$d_{\pi}(y) = \pi^{-1}(y). \quad (3-2)$$

[21]

Jedan primjer supstitucije može biti reverzni alfabet

$$a \rightarrow z, b \rightarrow y, \dots, z \rightarrow a$$

koji daje tablicu šifriranja

Tablica 3. 1 Supstitucijska šifra reverznim alfabetom

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

Korištenjem permutacije alfabeta prikazane u Tablici 3.1, poruka

ovo je poruka

se lako šifrira u

lel qv klifpz.

3.2.1 Matrica frekvencije bigrama

Matrica frekvencije bigrama je $n \times n$ matrica A čiji elementi a_{ij} imaju vrijednost učestalosti, odnosno frekvencije pojavljivanja i -tog simbola ispred j -tog simbola nekog alfabeta. Na primjer, neka je alfabetom

[a, b, c, d, e]

šifriran neki tekst i da je time dobiven šifrat

"aabcd ddab ddace addeca babcbdeba abcdba ebad".

Matrica frekvencije bigrama za dobiveni šifrat je

$$A = \begin{matrix} & a & b & c & d & e \\ \begin{matrix} a \\ b \\ c \\ d \\ e \end{matrix} & \begin{bmatrix} 2 & 5 & 1 & 2 & 1 \\ 4 & 0 & 3 & 2 & 0 \\ 1 & 1 & 0 & 2 & 1 \\ 3 & 1 & 0 & 4 & 2 \\ 1 & 2 & 1 & 0 & 0 \end{bmatrix} \end{matrix}$$

*"a**ab**cd dd**ab** ddace addeca **ba**bcbdeba **ab**cdba ebad"*

Iz matrice se može isčitati da je element a_{12} jednak 5 što je jednako broju ponavljanja bigrama *ab*. Ostale vrijednosti bigrama se također mogu naći u matrici *A*. Naravno ova se ideja može generalizirati i na veće alfabete. U sljedećem primjeru formirat će se matrica frekvencije bigrama za engleski alfabet. Ispitni tekst je:

"Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created equal... and that government of the people, by the people, for the people, shall not perish from the earth."

Tekst daje matricu frekvencije

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	1006	1007	1008	1009	1010	1011	1012	1013	1014	1015	1016	1017	1018	1019	1020	1021	1022	1023	1024	1025	1026	1027	1028	1029	1030	1031	1032	1033	1034	1035	1036	1037	1038	1039	1040	1041	1042	1043	1044	1045	1046	1047	1048	1049	1050	1051	1052	1053	1054	1055	1056	1057	1058	1059	1060	1061	1062	1063	1064	1065	1066	1067	1068	1069	1070	1071	1072	1073	1074	1075	1076	1077	1078	1079	1080	1081	1082	1083	1084	1085	1086	1087	1088	1089	1090	1091	1092	1093	1094	1095	1096	1097	1098	1099	1100	1101	1102	1103	1104	1105	1106	1107	1108	1109	1110	1111	1112	1113	1114	1115	1116	1117	1118	1119	1120	1121	1122	1123	1124	1125	1126	1127	1128	1129	1130	1131	1132	1133	1134	1135	1136	1137	1138	1139	1140	1141	1142	1143	1144	1145	1146	1147	1148	1149	1150	1151	1152	1153	1154	1155	1156	1157	1158	1159	1160	1161	1162	1163	1164	1165	1166	1167	1168	1169	1170	1171	1172	1173	1174	1175	1176	1177	1178	1179	1180	1181	1182	1183	1184	1185	1186	1187	1188	1189	1190	1191	1192	1193	1194	1195	1196	1197	1198	1199	1200	1201	1202	1203	1204	1205	1206	1207	1208	1209	1210	1211	1212	1213	1214	1215	1216	1217	1218	1219	1220	1221	1222	1223	1224	1225	1226	1227	1228	1229	1230	1231	1232	1233	1234	1235	1236	1237	1238	1239	1240	1241	1242	1243	1244	1245	1246	1247	1248	1249	1250	1251	1252	1253	1254	1255	1256	1257	1258	1259	1260	1261	1262	1263	1264	1265	1266	1267	1268	1269	1270	1271	1272	1273	1274	1275	1276	1277	1278	1279	1280	1281	1282	1283	1284	1285	1286	1287	1288	1289	1290	1291	1292	1293	1294	1295	1296	1297	1298	1299	1300	1301	1302	1303	1304	1305	1306	1307	1308	1309	1310	1311	1312	1313	1314	1315	1316	1317	1318	1319	1320	1321	1322	1323	1324	1325	1326	1327	1328	1329	1330	1331	1332	1333	1334	1335	1336	1337	1338	1339	1340	1341	1342	1343	1344	1345	1346	1347	1348	1349	1350	1351	1352	1353	1354	1355	1356	1357	1358	1359	1360	1361	1362	1363	1364	1365	1366	1367	1368	1369	1370	1371	1372	1373	1374	1375	1376	1377	1378	1379	1380	1381	1382	1383	1384	1385	1386	1387	1388	1389	1390	1391	1392	1393	1394	1395	1396	1397	1398	1399	1400	1401	1402	1403	1404	1405	1406	1407	1408	1409	1410	1411	1412	1413	1414	1415	1416	1417	1418	1419	1420	1421	1422	1423	1424	1425	1426	1427	1428	1429	1430	1431	1432	1433	1434	1435	1436	1437	1438	1439	1440	1441	1442	1443	1444	1445	1446	1447	1448	1449	1450	1451	1452	1453	1454	1455	1456	1457	1458	1459	1460	1461	1462	1463	1464	1465	1466	1467	1468	1469	1470	1471	1472	1473	1474	1475	1476	1477	1478	1479	1480	1481	1482	1483	1484	1485	1486	1487	1488	1489	14
---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	----

koja je dimenzija 26 x 26, a retci i stupci daju frekvencije bigrama prema parovima slova alfabetu poredanih prema uobičajenom, abecednom, redoslijedu. Važno je primjetiti kako su vektori za slova j , x i z (vodoravno i okomito) nulvektori što je logično pošto u tekstu nema slova j , x i z .

Promatrajući opet matricu A , sumu redova matrice prikazuje vektor $\mathbf{f}$ dobiven umnoškom $A\mathbf{u}$, gdje je $\mathbf{u} = [\mathbf{1} \ \mathbf{1} \ \mathbf{1} \ \mathbf{1} \ \mathbf{1}]^T$ pa vrijedi da je

$$A\mathbf{e} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = \mathbf{f}, \quad (3-3)$$

odnosno za slučaj s početka potpoglavlja,

$$A\mathbf{e} = \begin{bmatrix} 2 & 5 & 1 & 2 & 1 \\ 4 & 0 & 3 & 2 & 0 \\ 1 & 1 & 0 & 2 & 1 \\ 3 & 1 & 0 & 4 & 2 \\ 1 & 2 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 11 \\ 9 \\ 5 \\ 5 \\ 4 \end{bmatrix}.$$

Množenjem matrice A i jediničnog vektora $\mathbf{u}$ s desne strane zapravo se vrši zbrajanje elemenata po redovima, a zbroj elemenata retka je tada jedan element u vektoru frekvencija $\mathbf{f}$. Iz navedenog se primjera može isčitati da je prvi element $f_1 = 11$, odnosno da se slovo a ispred bilo kojeg slova pojavljuje 11 puta, a time je i ukupan broj ponavljanja a u tekstu također jednak 11. Isti broj se dobiva sumiraju li se elementi prvog stupca ($2+4+1+3+1 = 11$).

3.2.1 Primjena rastava na singularne vrijednosti

Prilikom kriptanalize šifri iz ovog poglavlja, jedna od metoda kriptanalitičara je analiza frekvencija simbola šifrata i usporedba rezultata s frekvencijama simbola otvorenog teksta. Druga metoda je pokušaj razdvajanja simbola šifrata na kategorije samoglasnika i suglasnika.

Neovisno koja se metoda koristila, nezaobilazan je alat rastava na singularne vrijednosti (*engl. Singular Value Decomposition, SVD*). Izvođenje SVD na matrici A dobiva se rastav na 3 druge matrice, od kojih svaka sadržava korisne informacije o šifriranom tekstu.

Za neku $m \times n$ matricu A , rastav na singularne vrijednosti definiran je kao

$$A = U\Sigma V^T, \quad (3-4)$$

gdje su elementi u_j u stupcima $m \times m$ matrice U svojstveni vektori od AA^T , elementi v_j u stupcima $n \times n$ matrice V svojstveni vektori od $A^T A$, a singularne vrijednosti r_j na dijagonali $m \times n$ matrice Σ su korijeni svojstvenih vrijednosti AA^T i $A^T A$ različitih od nule. Za rastav $n \times n$ matrice A vrijedi sljedeće:

$$\begin{aligned}
 A &= U\Sigma V^T \\
 &= [u_1 \quad u_2 \quad \dots \quad u_n] \begin{bmatrix} r_1 & & & \\ & r_2 & & \\ & & \ddots & \\ & & & r_n \end{bmatrix} \begin{bmatrix} y_1^T \\ y_2^T \\ \vdots \\ y_n^T \end{bmatrix} \\
 &= r_1 u_1 y_1^T + r_2 u_2 y_2^T + \dots + r_n u_n y_n^T.
 \end{aligned} \tag{3-5}$$

Matrica frekvencije bigrama A jednaka je konačnom redu dobivenom u (3-4). Prvi član reda,

$$r_1 u_1 y_1^T,$$

naziva se *aproksimacija prvog ranga*.

Pomoću *aproksimacije prvog ranga* moguće je izvući neke korisne informacije o matrici frekvencija bigrama A . Uzimajući u obzir (3-3) i jednakost

$$A\mathbf{e} = A^T \mathbf{e} = \mathbf{f}, \tag{3-6}$$

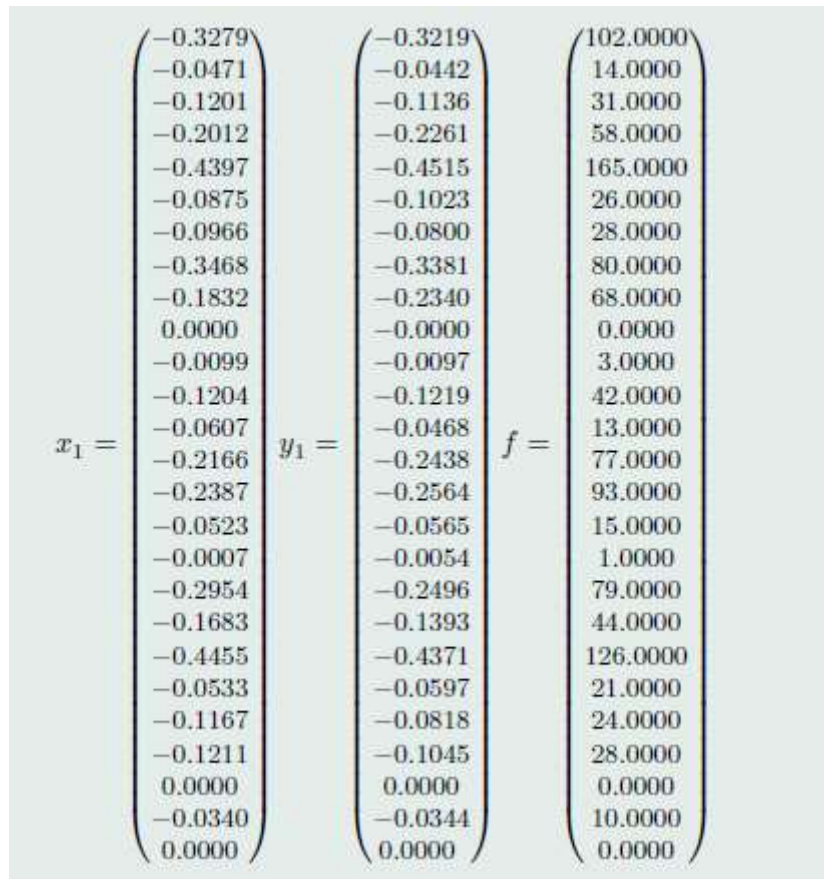
može se zapisati da je $A \approx r_1 u_1 y_1^T$ pa s time i

$$\begin{aligned}
 (r_1 u_1 y_1^T) \mathbf{e} &= (r_1 u_1 y_1^T)^T \mathbf{e} = \mathbf{f}, \\
 (r_1 u_1 y_1^T) \mathbf{e} &= (r_1 u_1 y_1^T) \mathbf{e} = \mathbf{f}.
 \end{aligned} \tag{3-7}$$

Izmjenom redoslijeda vrijedi i da je

$$(r_1 y_1^T \mathbf{e}) u_1 = (r_1 u_1^T \mathbf{e}) y_1 = \mathbf{f}. \tag{3-8}$$

U potonjoj jednadžbi, lijevi i desni singularni vektori su množeni skalarima $r_1 y_1^T \mathbf{e}$ i $r_1 u_1^T \mathbf{e}$. To znači da su u_1 i y_1 proporcionalni $\mathbf{f}$. Ova se metoda može konkretnije razraditi SVD rastavom matrice A dobivene iz ispitnog teksta iz potpoglavlja 3.2.1. Na Slici 3.1 uspoređeni su lijevi i desni singularni vektori s $\mathbf{f}$.



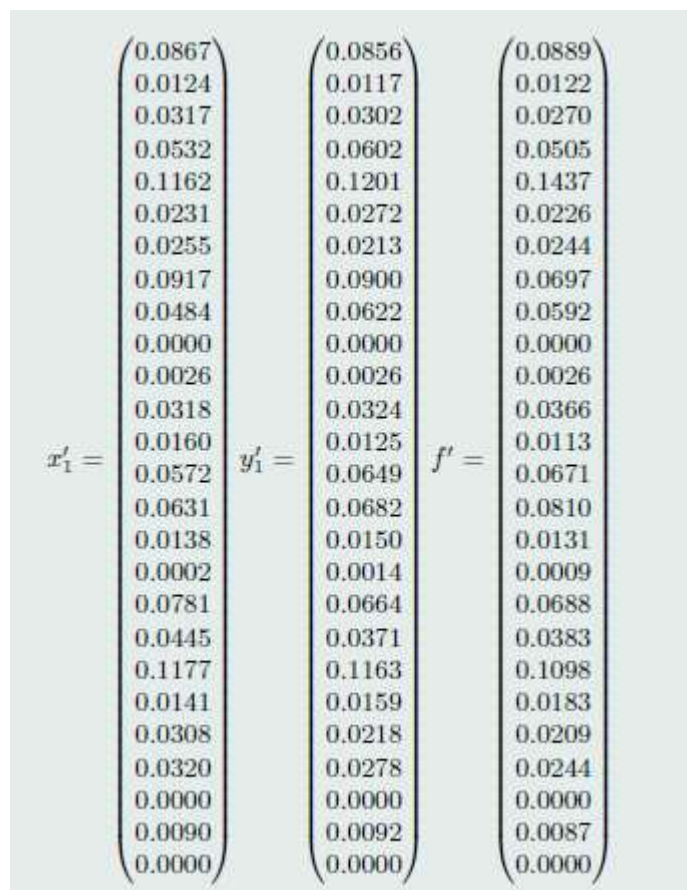
Slika 3. 2 Usporedba prvog lijevog i desnog singularnog vektora s frekvencijskim vektorom f

Vektori u_1 i y_1 pokazuju visoku korelaciju, dok vektor f ne pokazuje zamjetnu korelaciju s nijednim od navedenih vektora. Iz f se dakako može izvući informacija o odsutnosti slova j, x i z obilježena nulama u svim vektorima.

Za dobivanje relativne frekvencije pojedinih elemenata u vektoru potrebno je podijeliti svaki element sa sumom svih elemenata u vektoru:

$$\begin{aligned}
 x'_1 &= \frac{x_1}{\sum x_1} \\
 y'_1 &= \frac{y_1}{\sum y_1} \\
 f' &= \frac{f}{\sum f}
 \end{aligned}
 \tag{3-9}$$

Na taj način dobiveni su vektori sa Slike 3.2



Slika 3. 3 Usporedba frekvencija prvih lijevih i desnih singularnih vektora s vektorom frekvencija f

Sa Slike 3.2 vidljivo je kako vektori x' i y' blisko koreliraju s f' .

3.3 Kriptoanaliza Hillove šifre

Hilova šifra je vrsta polialfabetске supstitucijske šifre pošto se njome mogu šifrirati bigrami (slijed od dva slova nekog alfabeta, blok od dva slova), trigrami (slijed od tri slova nekog alfabeta, blok od tri slova) odnosno blokovi slova proizvoljne veličine. Prije samog šifriranja svih se l različitih slova otvorenog teksta zamjeni s l međusobno različitim pozitivnih cijelih brojeva. Jednostavnija shema zamjene slova engleskog alfabeta brojevima 0,...,25 prikazana je u Tablici 3.2.

Tablica 3. 2 Engleski alfabet i numerički ekvivalenti [21]

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ekvivalenti otvoreni tekst brojeva dijeli se u blokove veličine n te se time dobije konačan broj vektora $\mathbf{x}$ dimenzija n . Šifrirani vektor $\mathbf{y}_i$ dobiva se modulo l množenjem ključa K , predstavljen nesingularnom matricom $n \times n$, vektorom $\mathbf{x}_i$. Odnosno,

$$\mathbf{y}_i = K\mathbf{x}_i \pmod{l}. \quad (3-10)$$

Šifrirana $n \times n$ matrica Y (n stupaca matrice su zapravo n -dimenzionalni vektori $\mathbf{y}_i$) se po istom principu dobiva produktom ključa i matrice otvorenog teksta X (n stupaca matrice su zapravo n -dimenzionalni vektori $\mathbf{x}_i$) i vrijedi

$$Y = KX \pmod{l}. \quad (3-11)$$

Postupak dešifriranja je razumljivo tada

$$\mathbf{x}_i = K^{-1}\mathbf{y}_i \pmod{l}, \quad (3-12)$$

odnosno za slučaj s matricama

$$X = K^{-1}Y \pmod{l}. \quad (3-13)$$

Problem s kojim se susreće kriptanalitičar prilikom razbijanja Hillove šifre je određivanje matrice K , a time i matrice K^{-1} . Ako je došao u posjed dijela šifrata i pripadajućeg otvorenog teksta time je zapravo saznao dio vektora otvorenog teksta $\mathbf{x}$ i dio šifrata, odnosno šifriranih vektora $\mathbf{y}$. Postoji mogućnost formiranja invertibilne matrice $n \times n \pmod{l}$ uz poznavanje samo dijela otvorenog teksta. Tada se $K\mathbf{x}_i = \mathbf{y}_i$ može zapisati u obliku $K = \mathbf{y}_i\mathbf{x}_i^{-1}$ odakle se dobiva šifrska matrica – matrica ključa. Invertiranjem matrice ključa K modulo l dobiva se matrica za dešifriranje K^{-1} .

Uz poznavanje otvorenog teksta i pripadajućeg šifrata važno je i znati veličinu bloka n . Pretpostavka je da kriptanalitičar ima pristup komunikacijskom kanalu i da može prikupiti dovoljno uzoraka šifriranih poruka. Veličinu bloka moguće je odrediti jednostavnim pogađanjem, ako poruka nije predugačka. Na primjer, ako je prikupljen uzorak ZSHLFGLKTVDUWAQBCG s 18 simbola, tada 18 mora biti višekratnik veličine bloka – veličine 2, 3, 6, 9 ili 18. U slučaju da je veličina bloka 6, 9 ili 18 jednostavno broj simbola ne bi bio dovoljan za formiranje $\mathbf{x}_i$ i $\mathbf{y}_i$, a time ni određivanje matrice K i K^{-1} . Prilikom ove analize pretpostavlja se da je uz prikupljeni uzorak dodatno, iz nekih drugih izvora, dano njegovo značenje u otvorenom tekstu. Na primjeru neka je poruka koju nosi šifrat CRYPTOGRAPHYISCOOL.

Koristeći pretpostavku za veličinu bloka 2 i zamjenu iz Slike 3.1 određuje se da je poruka:

CRYPTOGRAPHYISCOOL ekvivalentno 2 17 24 15 19 14 6 17 0 15 7 24 8 18 2 14 14 11, te da se šifrira u ZSHLFGKTVDUWAQBCG što je ekvivalentno 25 18 7 11 5 6 11 10 19 21 3 20 22 0 16 1 2 6. Korištenjem vektorskog zapisa u blokovima vrijedi:

$$\begin{bmatrix} 2 \\ 17 \end{bmatrix} \rightarrow \begin{bmatrix} 25 \\ 18 \end{bmatrix} \quad \begin{bmatrix} 24 \\ 15 \end{bmatrix} \rightarrow \begin{bmatrix} 7 \\ 11 \end{bmatrix} \quad \begin{bmatrix} 19 \\ 14 \end{bmatrix} \rightarrow \begin{bmatrix} 5 \\ 6 \end{bmatrix} \quad \dots$$

Zadaća je konstruirati 2 x 2 matricu invertibilnu modulo 26 koristeći blokove otvorenog teksta. Ako se uzmu prva dva bloka i formira matrica, dobiva se

$$M = \begin{bmatrix} 2 & 24 \\ 17 & 15 \end{bmatrix},$$

čija determinanta $\det(M) = -378$ nije relativno prim prema 26, pa M nije invertibilna. Zamjenom drugog bloka u matrici M sa sljedećim blokom u redu vrijedi da je

$$M = \begin{bmatrix} 2 & 19 \\ 17 & 14 \end{bmatrix},$$

a determinanta $\det(M) = -295 \equiv 17 \pmod{26}$. Provjerom se može dokazati da je 17 modularni inverz broja 26 pa je time ovakva matrica M invertibilna. Sada, koristeći (3-2), vrijedi da je

$$K \begin{bmatrix} 2 & 19 \\ 17 & 14 \end{bmatrix} = \begin{bmatrix} 25 & 5 \\ 18 & 6 \end{bmatrix},$$

odnosno

$$K = \begin{bmatrix} 25 & 5 \\ 18 & 6 \end{bmatrix} \begin{bmatrix} 2 & 19 \\ 17 & 14 \end{bmatrix}^{-1} = \begin{bmatrix} 25 & 5 \\ 18 & 6 \end{bmatrix} \begin{bmatrix} 10 & 5 \\ 25 & 20 \end{bmatrix} = \begin{bmatrix} 11 & 17 \\ 18 & 2 \end{bmatrix}.$$

Da bi se odredila točnost ključa K mora se testirati na poznatom otvorenom tekstu CRYPTOGRAPHYISCOOL.

$$\begin{aligned} \mathbf{y}_i = K\mathbf{x}_i &= \begin{bmatrix} 11 & 17 \\ 18 & 2 \end{bmatrix} \begin{bmatrix} 2 \\ 17 \end{bmatrix}, \begin{bmatrix} 24 \\ 15 \end{bmatrix}, \begin{bmatrix} 19 \\ 14 \end{bmatrix}, \begin{bmatrix} 6 \\ 17 \end{bmatrix}, \begin{bmatrix} 0 \\ 15 \end{bmatrix}, \begin{bmatrix} 7 \\ 24 \end{bmatrix}, \begin{bmatrix} 8 \\ 18 \end{bmatrix}, \begin{bmatrix} 2 \\ 14 \end{bmatrix}, \begin{bmatrix} 14 \\ 11 \end{bmatrix} \\ &= \begin{bmatrix} 25 \\ 18 \end{bmatrix}, \begin{bmatrix} 25 \\ 20 \end{bmatrix}, \begin{bmatrix} 5 \\ 6 \end{bmatrix}, \begin{bmatrix} 17 \\ 12 \end{bmatrix}, \begin{bmatrix} 21 \\ 4 \end{bmatrix}, \begin{bmatrix} 17 \\ 18 \end{bmatrix}, \begin{bmatrix} 4 \\ 24 \end{bmatrix}, \begin{bmatrix} 0 \\ 12 \end{bmatrix}, \begin{bmatrix} 3 \\ 14 \end{bmatrix}. \end{aligned}$$

Vektori $\begin{bmatrix} 2 \\ 17 \end{bmatrix}$ i $\begin{bmatrix} 19 \\ 14 \end{bmatrix}$ su dobro šifrirani u vektore $\begin{bmatrix} 25 \\ 18 \end{bmatrix}$ i $\begin{bmatrix} 5 \\ 6 \end{bmatrix}$ pošto su oni i korišteni prilikom traženja ključa, ali ostatak šifrata ne odgovara šifratu kojeg kriptanalitičar ima u posjedu. Zaključak je da taj da veličina bloka nije 2. Drugi je izbor bio blok veličine 3. U tom slučaju matrica K je 3 x 3 matrica i vrijedi

$$K \begin{bmatrix} 2 & 15 & 6 & 15 & 8 & 14 \\ 17 & 19 & 17 & 7 & 18 & 14 \\ 24 & 14 & 0 & 24 & 2 & 11 \end{bmatrix} = \begin{bmatrix} 25 & 11 & 11 & 21 & 22 & 1 \\ 18 & 5 & 10 & 3 & 0 & 2 \\ 7 & 6 & 19 & 20 & 16 & 6 \end{bmatrix}.$$

Kao i u prethodnom slučaju, potrebno je odabrati n stupaca u matrici otvorenog teksta X koji će tvoriti invertibilnu $n \times n$ matricu. Gledajući posljednji redak matrice X , svi elementi osim zadnjeg (elementa 11) su parni, dakle koristit će se zadnji stupac. Pošto je element u zadnjem stupcu i prvom retku iste matrice paran broj, barem jedan od elementata preostala dva stupca u prvom retku mora sadržavati neparan broj. Prema tome za preostala dva stupca matrice vrijedi da ne smiju oba biti iz stupaca 1, 3 ili 5. Za prvi odabir matrica X će sadržavati stupce 1, 2 i 6 pa se dobiva matrica

$$M = \begin{bmatrix} 2 & 15 & 14 \\ 17 & 19 & 14 \\ 24 & 14 & 11 \end{bmatrix}.$$

Determinanta matrice M , $\det(M) = -791 \equiv 15 \pmod{26}$, potvrđuje da je matrica invertibilna. Prema tome

$$KM = K \begin{bmatrix} 2 & 15 & 14 \\ 17 & 19 & 14 \\ 24 & 14 & 11 \end{bmatrix} = \begin{bmatrix} 25 & 11 & 1 \\ 18 & 5 & 2 \\ 7 & 6 & 6 \end{bmatrix}$$

I tada je

$$K = \begin{bmatrix} 25 & 11 & 1 \\ 18 & 5 & 2 \\ 7 & 6 & 6 \end{bmatrix} \begin{bmatrix} 2 & 15 & 14 \\ 17 & 19 & 14 \\ 24 & 14 & 11 \end{bmatrix}^{-1} = \begin{bmatrix} 25 & 11 & 1 \\ 18 & 5 & 2 \\ 7 & 6 & 6 \end{bmatrix} \begin{bmatrix} 13 & 9 & 24 \\ 3 & 12 & 14 \\ 8 & 10 & 15 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{bmatrix}.$$

Dobiveni ključ provjerava se na paru *šifrat-otvoreni tekst*. Dobiva se

$$\begin{bmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{bmatrix} \begin{bmatrix} 2 & 15 & 6 & 15 & 8 & 14 \\ 17 & 19 & 17 & 7 & 18 & 14 \\ 24 & 14 & 0 & 24 & 2 & 11 \end{bmatrix} = \begin{bmatrix} 25 & 11 & 11 & 21 & 22 & 1 \\ 18 & 5 & 10 & 3 & 0 & 2 \\ 7 & 6 & 19 & 20 & 16 & 6 \end{bmatrix}$$

što odgovara šifranom otvorenom tekstu i potvrđuje ispravnost ključa K .

3.4 Kriptoanaliza kongurentnih kriptosustava s javnim ključem

Kongurentni kriptosustavi s javnim ključem jednostavan su model kriptosustava s javnim ključem koji danas imaju široku uporabu u svim ozbiljnijim oblicima sigurnih komunikacija. Zanimljivo je da ovaj model kriptosustava ima određena svojstva povezana s tzv. **mrežastim strukturama** (*engl. Lattice*) dimenzija 2. Male dimenzije strukture čine ovaj kriptosustav ranjivim na naprednije metode kriptoanalize.

3.4.1 Korištenje kongurentnih kriptosustava s javnim ključem

Pošiljatelj započinje kriptiranje odabirom relativno velikog prirodnog broja q , koji će se koristiti kao javni parametar, i odabirom dva prirodna broja f i g koji će ostati tajni. Tajni parametri moraju zadovoljavati:

$$f < \sqrt{\frac{q}{2}}, \quad \sqrt{\frac{q}{4}} < g < \sqrt{\frac{q}{2}} \quad i \quad \text{nzd}(f, q) = 1.$$

Pošiljatelj tada računa sljedeću vrijednost:

$$h \equiv f^{-1} g \pmod{q}, \quad 0 < h < q. \quad (3-14)$$

Sada pošiljatelj posjeduje privatni ključ u obliku para brojeva f i g (po iznosu relativno mali prirodni brojevi) i javni ključ h (po iznosu relativno veliki prirodni broj).

Kriptiranje se vrši odabirom otvorenog teksta m i slučajnog broja $r \in \mathbb{N}$ (jednokratni ključ) koji zadovoljava nejednakosti

$$0 < m < \sqrt{\frac{q}{4}} \quad i \quad 0 < r < \sqrt{\frac{q}{2}}.$$

Šifrat se dobiva izračunom

$$e = rh + m \pmod{q}, \quad 0 < e < q. \quad (3-15)$$

Primalac dobiva šifrat i najprije određuje

$$a \equiv fe \pmod{q}, \quad 0 < a < q \quad (3-16)$$

i nakon toga otvoreni tekst dobiva iz

$$b \equiv f^{-1} a \pmod{g}, \quad 0 < b < g. \quad (3-17)$$

Važno je istaknuti da je f^{-1} iz (3-17) zapravo inverz f modulo g . Nadalje se može potvrditi kako je doista $b = m$ i to najprije određivanjem da a zadovoljava sljedeće:

$$a \equiv fe \equiv f(rh + m) \equiv frf^{-1}g + fm \equiv rg + fm \pmod{q}.$$

Ograničenja na veličine brojeva f, g, r, m navode da je i zbroj produkata $rg + fm$ zapravo još uvijek relativno mali broj:

$$rg + fm < \sqrt{\frac{q}{2}}\sqrt{\frac{q}{2}} + \sqrt{\frac{q}{2}}\sqrt{\frac{q}{4}} < q.$$

Stoga kada primalac odredi $a \equiv fe \pmod{q}$ uz $0 < a < q$, dobiva točno određenu vrijednost

$$a = rg + fm \quad (3-18)$$

Što je jednadžba cijelih brojeva s lijeve i desne strane jednakosti, a ne kongurencija modulo q . Na kraju primalac dekriptiranjem dobiva:

$$b \equiv f^{-1}a \equiv f^{-1}(rg + fm) \equiv f^{-1}fm = m \pmod{g}, \quad 0 < b < g.$$

Kako je $m < \sqrt{q/4} < g$, evidentno je tada i $b = m$.

Konkretniji prikaz ovog kriptosustava najlakše je ostvariti korištenjem konkretnih brojeva. Neka primalac na primjer odabere

$$q = 122430513841, \quad f = 231231 \quad \text{i} \quad g = 195698.$$

Može se vidjeti da su $f \approx 0.66\sqrt{q}$ i $g \approx 0.56\sqrt{q}$ unutar dozvoljenih granica. Primalac računa

$$f^{-1} \equiv 49194372303 \pmod{q} \quad \text{i} \quad h \equiv f^{-1}g \equiv 39245579300 \pmod{q}.$$

Time je dobio par brojeva $(q, h) = (122430513841, 39245579300)$ koji će se koristiti kao javni ključ.

Pošiljatelj dobiva javni ključ i odluči poslati određenu tajnu poruku nazad. Neka je otvoreni tekst poruke $m = 123456$ i uz to odabere neki slučajni broj $r = 101010$. Koristi primaočev javni ključ da dobije šifrat e na sljedeći način:

$$e \equiv rh + m \equiv 18357558717 \pmod{q}.$$

Primalac dekriptira poruku korištenjem svojeg privatnog ključac f . Najprije računa

$$a \equiv fe \equiv 48314309316 \pmod{q}.$$

Zatim koristi vrijednost $f^{-1} \equiv 193495 \pmod{g}$ da dobije poruku u otvorenom tekstu na način:

$$f^{-1}a \equiv 193495 \cdot 48314309316 \equiv 123456 \pmod{g}.$$

3.4.2 Kriptoanaliza kongurentnih kriptosustava s javnim ključem

Kriptoanalitičar bi za pronalaženje privatnog ključa ili otvorenog teksta mogao koristiti metodu uzastopnih pokušaja (*engl. Brute-force*), ali takva metoda iziskuje $\mathcal{O}(q)$ operacija. Zanimljivije je promotriti pokušaj otkrivanja privatnog ključa (f, g) na temelju poznatog javnog

ključa (q, h) . Zadatak je kriptanalitičara pronalazak bilo kojeg para brojeva $F, G \in \mathbb{N}$ koji zadovoljava:

$$Fh \equiv G \pmod{q} \quad i \quad F = \mathcal{O}(\sqrt{q}) \quad i \quad G = \mathcal{O}(\sqrt{q}), \quad (3-19)$$

tada bi se par (F, G) mogao koristiti kao ključ za dekriptiranje. Zapisujući kongurenciju (3-19) kao $Fh = G + qR$, problem se preformulirao u zadatak pronalaska komparativno malih cijelih brojeva (F, G) sa svojstvom

$$F(1, h) - R(0, q) = (F, G). \quad (3-20)$$

Problem je sada sveden na traženje linearne kombinacije $\mathbf{w} = a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2$ na temelju poznatih vektora $\mathbf{v}_1 = (1, h)$ i $\mathbf{v}_2 = (0, q)$ duljine $\mathcal{O}(q)$ te poznate duljine vektora $|\mathbf{w}| = \mathcal{O}(\sqrt{q})$, koeficijenti a_1 i a_2 su cijeli brojevi. Prema tome kriptanalitičar mora pronaći vektor kojemu je modul mali broj različit od nule i pripada skupu vektora

$$L = \{a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 : a_1, a_2 \in \mathbb{Z}\}.$$

Skup L je primjer jedne dvodimenzionalne mrežaste strukture. U suštini dvodimenzionalni vektorski prostor s bazom $(\mathbf{v}_1, \mathbf{v}_2)$ nad kojim su dozvoljene linearne kombinacije sa skalarima iz skupa cijelih brojeva.

Na kongurentni kriptosustav s javnim ključem iz Poglavlja 3.4.1 moguće je primijeniti algoritam Gaussove redukcije rešetke. U primjeru iz prethodnog poglavlja javni je ključ bio par brojeva

$$(q, h) = (122430513841, 39245579300).$$

Gaussovim se algoritmom reducira rešetka čiji su vektori baze, primjenom (3-20),

$$\mathbf{v}_1 = (1, 39245579300) \quad i \quad \mathbf{v}_2 = (0, 122430513841).$$

Provođenjem algoritma u 11 iteracija, dobiva se najmanja moguća baza koju čine vektori

$$(-231231, -195698) \quad i \quad (-368222, 217835).$$

Uz zanemarivanje predznaka, kriptanalitičar je uspješno pronašao privatni ključ $f = 231231$ i slučajno odabrani broj $g = 195698$.

4. Zaključak

Linearna algebra, kao matematička disciplina koja se između ostalog bavi vektorskim prostorima i linearnim transformacijama, svakodnevno pronalazi sve širu primjenu unutar drugih prirodnih, tehničkih i društvenih znanosti. Iako možda svi problemi u kojima se primjenjuje nisu linearne prirode, mnogi algoritmi iz linearne algebre daju dobre aproksimacije rezultata. Za bilo koji slučaj vrijedi da se razvijeni algoritmi vrlo lako mogu implementirati u digitalna računala koja su danas uz ljudsku inovativnost osnovni faktori napretka znanosti i tehnologije.

Kriptoanaliza je svoj veliki razvoj dostigla primjenom u mnogobrojnim ratovima kroz ljudsku povijest kada je sigurnost prenošenih informacija donosila stratešku prednost, ali ponekad i pitanje života ili smrti čitavih naroda. U mirnodobnom razdoblju kriptoanaliza, odnosno analiziranje ranjivosti kriptosustava, pronašla je svoju primjenu u gotovo svim tipovima suvremenih digitalnih komunikacija, u očuvanju tajnosti podataka itd.

LITERATURA

- [1] M. Stamp, R. M. Low - Applied Cryptanalysis, Breaking Ciphers in the Real World (Wiley, New Jersey [USA], 2007.)
- [2] H. F. Gaines - Cryptanalysis, A study of ciphers and their solution (Dover, New York [USA], 1956.)
- [3] J. Hoffstein, J. Pipher, J. H. Silverman - An Introduction to Mathematical Cryptography (Springer, New York [USA], 2008.)
- [4] J. Katz, Y. Lindell - Introduction to Modern Cryptography (CRC Press, 2007.)
- [5] A. Menezes, P. C. van Oorschot, S. A. Vanstone - Handbook of Applied Cryptography (CRC Press, 1996.)
- [6] K. Ruohonen - Mathematical Cryptology (*e-book*, 2014.)
- [7] G. V. Bard - Algebraic Cryptanalysis (Springer, 2009.)
- [8] A. Dujella, M. Maretić - Kriptografija (Element, Zagreb, 2007.)
- [9] G. V. Bard - Algorithms for solving linear and polynomial systems of equations over finite fields with application to cryptanalysis (*doktorska disertacija, University of Maryland*, 2007.)
- [10] M. Eisenberg - Hill Ciphers and Modular Linear Algebra (*skripta, University of Massachusetts*, 1999.)
- [11] T. E. Schilling - Towards Efficient Algorithms in Algebraic Cryptanalysis (*doktorska disertacija, University of Bergen*, 2012.)
- [12] K. H. Rosen - Elementary Number Theory and Its Application (Addison-Wesley, 1986.)
- [13] T. Honn, S. Stone - SVD and Cryptograms, Linear Algebra (*predavanja s WEB-a, College of the Redwood*, 2002.)
- [14] Gilbert Strang - Introduction to Linear Algebra, 3rd Ed. (Wellesley-Cambridge press, 2013.)

- [15] S. Lipschutz, M. L. Lipson - Schaum's Outlines: Linear Algebra (McGraw-Hill, 2009.)
- [16] Gilbert Strang - Linear Algebra and Its Application, 4th Ed. (Thomson Brooks/Cole publication, 2006.)
- [17] Jim Hefferon - Linear Algebra (*open-source book*, <http://joshua.smcvt.edu/linearalgebra>)
- [18] V. Hari - Linearna Algebra (*skripta PMF-a*, Zagreb, 2005.)
- [19] K. Horvatić - Linearna algebra (Golden marketing – Tehnička knjiga, Zagreb, 2003.)
- [20] C. D. Meyer - Matrix Analysis and Applied Linear Algebra (Siam, 2001.)
- [21] Adriana Đuraković – Klasična kriptografija (*Diplomski rad*, Osijek, 2014.)
- [22] <http://crypto.interactive-maths.com/>
- [23] <https://web.math.pmf.unizg.hr/nastava/la/dodatno.html>

Sažetak

Sa željom, i potrebom, da se održi tajnost spremljenih ili prenošenih informacija intenzivno se razvijaju nove metode kriptiranja tih podataka. Bilo da je pitanje osobnih, državnih ili poslovnih informacija, u krivim rukama one potencijalno mogu značiti veliku štetu. Kriptoanaliza ima zadaću pronalaženje ranjivosti kriptosustava te na temelju novih saznanja razvijati nove pouzdanije kriptografske algoritme.

Kako su suvremene komunikacije najvećim dijelom digitalne, obrađivane preko računala, time su i algoritmi kriptografije razvijani sa idejom konačne implementacije na računalu. Samim time je i pristup kriptoanalizi predodređen računalom, ali i neophodan zbog potrebe za izvođenjem velikog broja aritmetičkih i logičkih operacija u što kraćem vremenu.

Primjenom linearne algebre i nekih algoritama baziranih na vektorskoj analizi moguće je uvelike smanjiti broj operacija potrebnih da se pronađe rješenje problema. Kako je već i spomenuto u radu sami algoritmi vezani za analizu matičnih sustava, vektora i njihovih svojstava lako se implementiraju na računalima.

Summary

With will, and need, to preserve secrecy of information that one wants to transmit or permanently save there is always an intense research on developing new methods for data encryption. Whether the information is personal, statesmanlike or military in nature, fallen in the wrong hands it can potentially mean harm. Cryptanalysis has the task of finding a vulnerability in cryptosystems to gain new knowledge for implementation and development of more reliable cryptographic algorithms.

As modern communications are mostly digital, processed via computer, thus cryptography and algorithms have to be developed with the idea of the final implementation on the computer. Therefore the approach to cryptanalysis is predetermined to a computer, but also necessary because of the need to perform a large number of arithmetic and logical operations in the shortest possible time.

Applying linear algebra and some algorithms based on vector analysis it is possible to greatly reduce the number of operations required to find a solution to the problem. As already mentioned in the work, algorithms related with analysis of matrix systems, vectors and their properties are easily implemented on computers.

Životopis

Darko Brežnjak rođen je 11. listopada 1991. u Varaždinu. Osnovnu školu pohađa od 1997. do 2006. godine u Lepoglavi. Po završetku osnovne škole upisuje srednju Elektrostrojarsku školu u Varaždinu, smjer Elektrotehničar. Tijekom srednje škole aktivno sudjeluje u programu Centra izvrsnosti iz fizike Varaždinske županije te sudjeluje na državnom natjecanju eksperimentalnih radova iz fizike 2010. godine. Iste te godine završava srednju školu te se upisuje na preddiplomski stručni studij elektrotehnike pri Tehničkom veleučilištu u Zagrebu. Po završetku stručnog studija 2013. godine stječe titulu stručnog prvostupnika inženjera elektrotehnike (bacc. ing. el.).

Nakon polaganja razlikovnih ispita 2014. godine upisuje izvanredni diplomski studij elektrotehnike na Elektrotehničkom fakultetu u Osijeku, smjer komunikacije i informatika.

vlastoručni potpis