Primjene linearne algebre u kriptoanalizi

Brežnjak, Darko

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 kriptoanalizi
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 kriptoanalizi**

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

1. UVOD

Linearna algebra te matematički alati koji su razvijeni njenom primjenom u prirodnim i tehničkim znanostima našli su svoju primjenu i u krtiptologiji. 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 algebra u grani kriptologije koja se, između ostalog, bavi analizom kriptografskih sustava – kriptoanaliza.

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 kriptoanalize, ali i razrađuju konkretni primjeri kriptoanalitičkih napada baziranih na primjenama linearne algebre.

2. LINEARNA ALGEBRA

Osnovni zadatak linearne algebre je traženje rješenja sustava linearnih jednadžbi odnosno m x n linearnog sustava gdje m označava broj jednadžbi, a n broj nepoznanica sadržanih u jednadžbama sustava. *Linearna jednadžba* sa nepoznanicama $x_1, \dots, x_n$ je jednadžba koja se može zapisati u obliku

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{2-1}$$

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

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

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

$$A\boldsymbol{x} = \boldsymbol{b}, \tag{2-3}$$

gdje je A matrica koeficijenata a_{mn}, $\boldsymbol{x}$ vektor čije su komponente nepoznanice x_n te $\boldsymbol{b}$ 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

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

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 $\boldsymbol{M_{mn}}$. Operacija se provodi zbrajanjem „član po član“, to jest međusobno se zbroje elementi matrica s istim indeksom pa vrijedi

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

odnosno

$$A + B = C. \tag{2-6}$$

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 $A \in \boldsymbol{M_{mn}}$ skalarom $\lambda \in \mathbb{R}$ vrši se na način da skalar množi svaki element matrice pa je

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

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 skalarnom množenju,
(5) Jedinični element: $1A = A$.

Matrica dimenzije *m* x *n* množi se vektorom dimenzije *n* po principu skalarnog umnoška vektora pa vrijedi:

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

odnosno

$$A\boldsymbol{x} = \boldsymbol{b}. \tag{2-9}$$

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

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

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

Množenje matrice *A* dimenzija *m* x *n* s matricom *B* dimenzija *n* x *p* daje kao rezultat matricu *C* dimenzija *m* x *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 „ · “.

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

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*.

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

$$b_{11} \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} + b_{21} \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} + \cdots + b_{n1} \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix} = \begin{bmatrix} c_{11} \\ c_{21} \\ \vdots \\ c_{m1} \end{bmatrix} = \boldsymbol{c_1},$$

$$b_{12} \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} + b_{22} \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} + \cdots + b_{n2} \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix} = \begin{bmatrix} c_{12} \\ c_{22} \\ \vdots \\ c_{m2} \end{bmatrix} = \boldsymbol{c_2},$$

$$\vdots$$

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

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

Još jedna važna operacija nad matrica 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,

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

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) Jedinična 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 $\boldsymbol{a}^T\boldsymbol{b} = \boldsymbol{b}^T\boldsymbol{a}$.

2.1.2 Determinante

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

$$det : A \to \mathbb{R}, \tag{2-13}$$

je realan broj. Osim oznake det, determinanta se često označava vertikalnim crtama $|\ \ |$ 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:

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

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

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

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

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

ili pak razvojem po j-tom stupcu preko

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

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-Cauchyjev teorem*).

2.1.3 Inverz matrice

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

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

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

$$X_1 = X_1 I = X_1(AX_2) = (X_1A)X_2 = IX_2 = X_2$$

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 predočiti zapisom

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

2.2 Vektorski prostor i potprostor

Skup svih matrica $\boldsymbol{M_{mn}}$ uz operacije zbrajanja matrica i množenja skalara i matrice čini **vektorski prostor**.

Definicija 2.2.1 Neka je V neprazan skup na kojem su zadane binarna operacija zbrajanja $+: V \times V \to V$ i operacija množenja skalarima iz polja $\mathbb{H}$, $\cdot : \mathbb{H} \times V \to V$. 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) $1 \cdot a = 1,\ \forall a \in V$. *[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 skalara, 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) $(\forall \boldsymbol{x}, \boldsymbol{y} \in Z)(\forall \alpha, \beta \in \mathbb{R}) \quad \alpha\boldsymbol{x} + \beta\boldsymbol{y} \in Z.$

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 3x3 sustav:

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

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

$$4y + z = 2.$$

I takav se sustav može zapisati u matričnom obliku te se dobiva sustav $A\boldsymbol{x} = \boldsymbol{b}$

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

Iz matrice se koeficijenata, 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:

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

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

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

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

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

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

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

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

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

$$\boldsymbol{q}_1 = \frac{\boldsymbol{a}_1}{\|\boldsymbol{a}_1\|},$$

$$\boldsymbol{q}_2 = \frac{\overline{\boldsymbol{a}_2}}{\|\overline{\boldsymbol{a}_2}\|}, \qquad \overline{\boldsymbol{a}_2} = \boldsymbol{a}_2 - (\boldsymbol{q}_1 \cdot \boldsymbol{a}_2)\boldsymbol{q}_1,$$

$$\boldsymbol{q}_3 = \frac{\overline{\boldsymbol{a}_3}}{\|\overline{\boldsymbol{a}_3}\|}, \qquad \overline{\boldsymbol{a}_3} = \boldsymbol{a}_3 - (\boldsymbol{q}_1 \cdot \boldsymbol{a}_3)\boldsymbol{q}_1 - (\boldsymbol{q}_2 \cdot \boldsymbol{a}_3)\boldsymbol{q}_2,$$

$$\vdots$$

$$\boldsymbol{q}_n = \frac{\overline{\boldsymbol{a}_n}}{\|\overline{\boldsymbol{a}_n}\|}, \qquad \overline{\boldsymbol{a}_n} = \boldsymbol{a}_n - \sum_{i=1}^{n-1} (\boldsymbol{q}_i \cdot \boldsymbol{a}_n)\boldsymbol{q}_i .$$

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

$$A = \widehat{U}\begin{bmatrix}\Sigma\\0\end{bmatrix}V^* = \widehat{U}\Sigma V^*, \tag{2-20}$$

gdje je:

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

Stupci matrice $\widehat{U}$ 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 rešteke 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 $\boldsymbol{v_1}$ i $\boldsymbol{v_2}$ tako da vrijedi da je $\|\boldsymbol{v_1}\| < \|\boldsymbol{v_2}\|$. Algoritam sada nalaže, dok god je to moguće, reduciranje vektora baze $\boldsymbol{v_2}$ za višekratnike drugog vektora baze, $\boldsymbol{v_1}$. Za slučaj da je dozvoljeno oduzimanje proizvonjog višekratnika $\boldsymbol{v_1}$, tada se vektor $\boldsymbol{v_2}$ zamjenjuje vektorom

$$\boldsymbol{v_2^*} = \boldsymbol{v_2} - \frac{\boldsymbol{v_1} \cdot \boldsymbol{v_2}}{\|\boldsymbol{v_1}\|^2}\boldsymbol{v_1}$$

koji je okomit na vektor $\boldsymbol{v_1}$. Postupak zapravo daje novi vektor $\boldsymbol{v_2^*}$ koji je projekcija vektora $\boldsymbol{v_2}$ na pravac (ili na ravninu u općenitom slučaju) okomit s $\boldsymbol{v_1}$.

Za slučaj da je rešetka L sačinjena od samo pozitivnih cijelobrojnih parova, vektor $\boldsymbol{v_2^*}$ ne mora nužno biti unutar rešetke. U praksi se dozvoljava oduzimanje samo cijelobrojnih višekratnika $\boldsymbol{v_2}$ od vektora $\boldsymbol{v_2}$. Stoga se vektor $\boldsymbol{v_2}$ zamijenjuje vektorom

$$\boldsymbol{v_2} - m\boldsymbol{v_1} \quad za \quad m = \left\lfloor \frac{\boldsymbol{v_1} \cdot \boldsymbol{v_2}}{\|\boldsymbol{v_1}\|^2} \right\rceil,$$

gdje oznaka $\lfloor x \rceil$ određuje zaokruživanje dobivenog realnog rješenja na najbliži cijeli broj. Ako je primjenom algoritma vektor $\boldsymbol{v_2}$ i dalje veći, algoritam staje. Inače, izvrši se zamjena $\boldsymbol{v_1}$ i $\boldsymbol{v_2}$ 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 kriptoanalitičara krađa informacija koje razmjenjuju pošiljatelj 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 (pošiljatelj) i sugovornik (primatelj) imaju unaprijed dogovoren standard poruka kojima će komunicirati. U kriptografiji se takav oblik poruka naziva otvoreni tekst. Prema tome o*tvoreni tekst* je naziv za izvorni tekst koji pošiljatelj želi poslati primatelju, a da na njega nije primjenio šifriranje. Ako pošiljatelj želi sakriti informaciju sadržanu u poruci, primjenom postupka šifriranja dobiti će š*ifrat* (*njem. Das Chiffrat*) - 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.

Definicija 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* $e_k: \mathcal{P} \to \mathcal{C}$ *i* $d_k: \mathcal{C} \to \mathcal{P}$ *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, kriptoanalizu 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, …, 25. Za svaku permutaciju* $\pi \in \mathcal{K}$ *definira se*

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

i

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

[21]

Jedan primjer supstitucije može biti reverzni alfabet

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

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* x *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

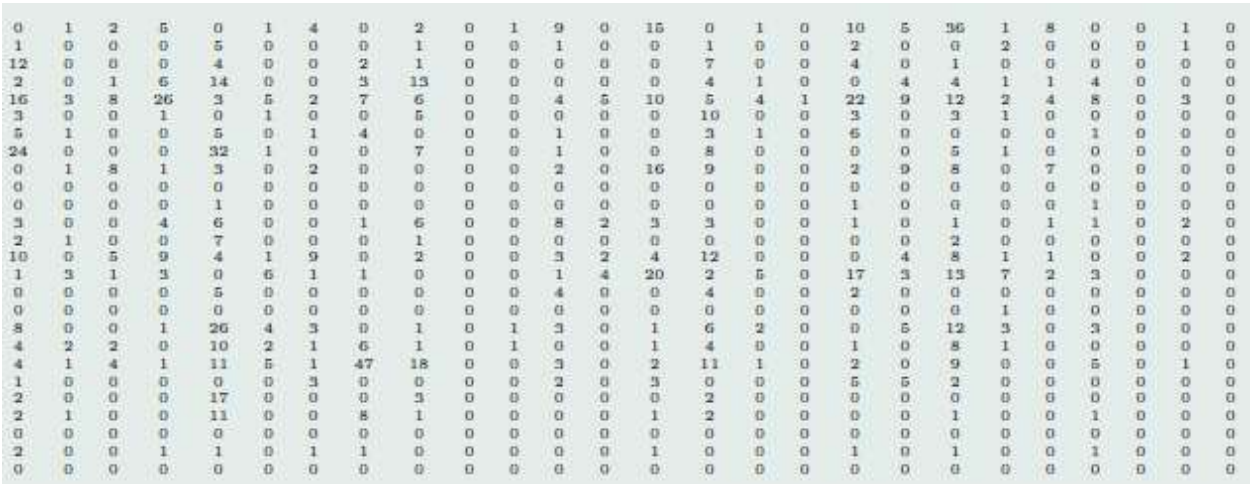
$$A = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{bmatrix} 2 & 5 & 1 & 2 & 1 \\ 4 & 0 & 3 & 2 & 0 \\ 1 & 1 & 0 & 2 & 1 \\ 3 & 1 & 0 & 4 & 2 \\ 1 & 2 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

"aabcd ddab ddace addeca babcbdeba abcdba ebad"

Iz matrice se može isčitati da je element a_{12} jednak 5 što je jednko 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



Slika 3. 1 Matrica frekvencija bigrama

koja je dimenzija 26 x 26, a retci i stupci daju frekvencije bigrama prema parovima slova alfabeta 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 $\boldsymbol{f}$ dobiven umnoškom $A\boldsymbol{u}$, gdje je $\boldsymbol{u} = [\mathbf{1} \quad \mathbf{1} \quad \mathbf{1} \quad \mathbf{1} \quad \mathbf{1}]^{\boldsymbol{T}}$ pa vrijedi da je

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

odnosno za slučaj s početka potpoglavlja,

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

Množenjem matrice *A* i jediničnog vektora $\boldsymbol{u}$ s desne strane zapravo se vrši zbrajanje elemenata po redovima, a zbroj elemenata retka je tada jedan element u *vektoru frekvencija* $\boldsymbol{f}$. 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 kriptoanalize šifri iz ovog poglavlja, jedna od metoda kriptoanalitičara 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* x *n* matricu *A*, rastav na singularne vrijednosti definiran je kao

$$A = U\Sigma V^T, \tag{3-4}$$

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

$$\begin{aligned} A &= U\Sigma V^T \\ &= [u_1 \quad u_2 \quad \cdots \quad u_n] \begin{bmatrix} r_1 & & & \\ & r_2 & & \\ & & \ddots & \\ & & & r_n \end{bmatrix} \begin{bmatrix} y_1^T \\ y_2^T \\ \vdots \\ y_n^T \end{bmatrix} \\ &= r_1u_1y_1^T + r_2u_2y_2^T + \cdots + r_nu_ny_n^T. \end{aligned} \tag{3-5}$$

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

$$r_1u_1y_1^T,$$

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

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

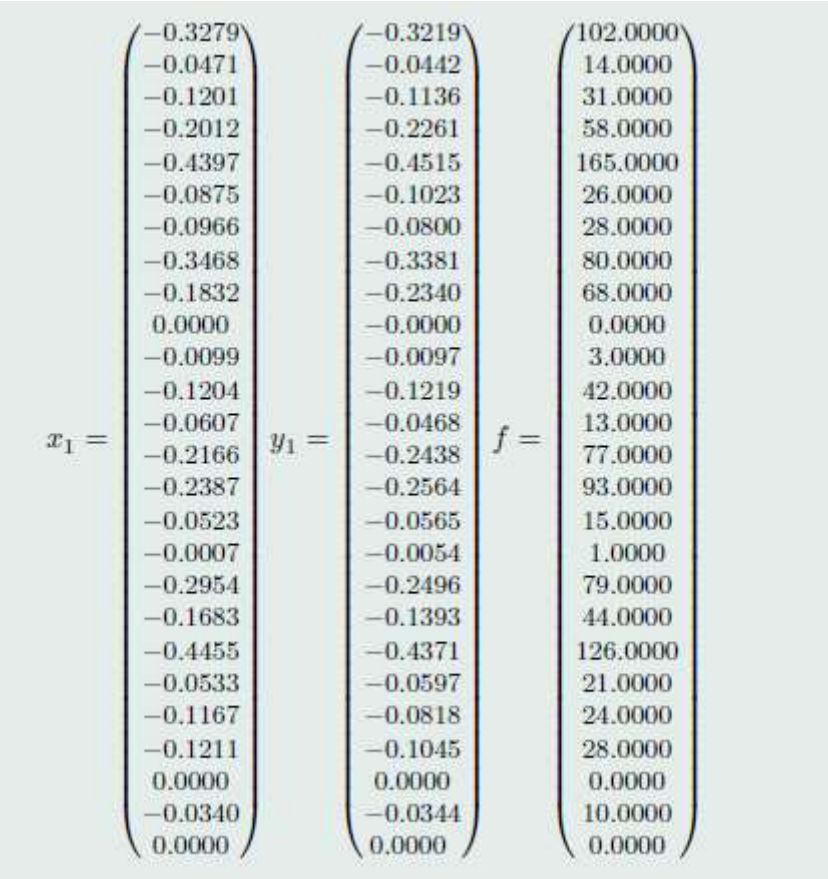
može se zapisati da je $A \approx r_1u_1y_1^T$ pa s time i

$$\begin{aligned} (r_1u_1y_1^T)\boldsymbol{e} = (r_1u_1y_1^T)^T\boldsymbol{e} = \boldsymbol{f}, \\ (r_1u_1y_1^T)\boldsymbol{e} = (r_1u_1y_1^T)\boldsymbol{e} = \boldsymbol{f}. \end{aligned} \tag{3-7}$$

Izmjenom redoslijeda vrijedi i da je

$$(r_1y_1^Te)u_1 = (r_1u_1^Te)y_1 = \boldsymbol{f}. \tag{3-8}$$

U potonjoj jednadžbi, lijevi i desni singularni vektori su množeni skalarima $r_1y_1^Te$ i $r_1u_1^Te$. To znači da su u_1 i y_1 proporcionalni $\boldsymbol{f}$. 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 $\boldsymbol{f}$.



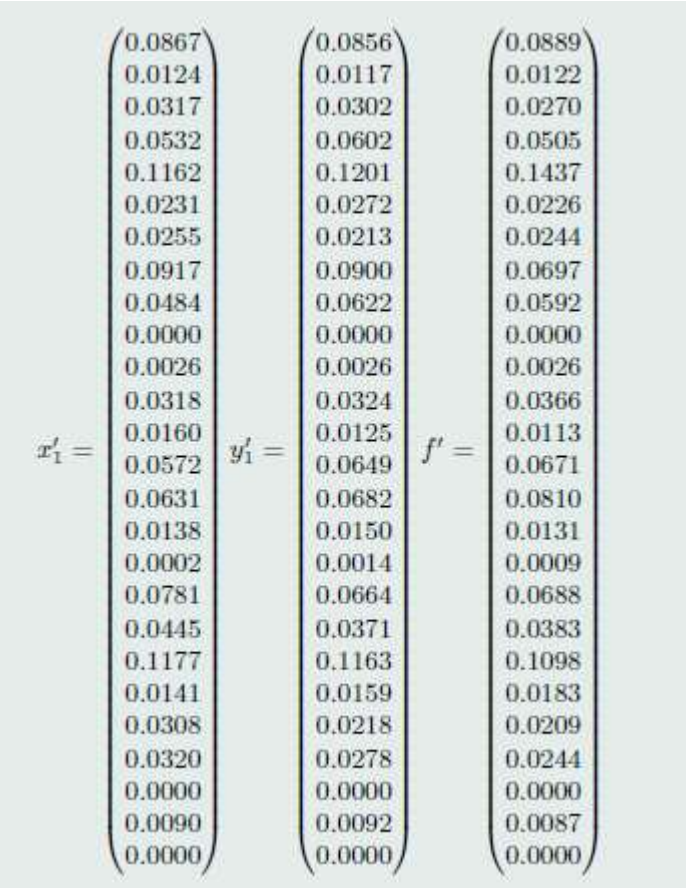
*Slika 3. 2 Usporedba prvog lijevog i desnog singularnog vektora s frekvencijskm vektorom **f***

Vektori u_1 i y_1 pokazuju visoku korelaciju, dok vektor $\boldsymbol{f}$ ne pokazuje zamjetnu korelaciju s nijednim od navedenih vektora. Iz $\boldsymbol{f}$ 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:

$$x_1' = \frac{x_1}{\sum x_1}$$
$$y_1' = \frac{y_1}{\sum y_1} \qquad (3\text{-}9)$$
$$f' = \frac{f}{\sum f}$$

Na taj način dobiveni su vektori sa Slike 3.2



$$x_1' = \begin{pmatrix} 0.0867 \\ 0.0124 \\ 0.0317 \\ 0.0532 \\ 0.1162 \\ 0.0231 \\ 0.0255 \\ 0.0917 \\ 0.0484 \\ 0.0000 \\ 0.0026 \\ 0.0318 \\ 0.0160 \\ 0.0572 \\ 0.0631 \\ 0.0138 \\ 0.0002 \\ 0.0781 \\ 0.0445 \\ 0.1177 \\ 0.0141 \\ 0.0308 \\ 0.0320 \\ 0.0000 \\ 0.0090 \\ 0.0000 \end{pmatrix} \quad y_1' = \begin{pmatrix} 0.0856 \\ 0.0117 \\ 0.0302 \\ 0.0602 \\ 0.1201 \\ 0.0272 \\ 0.0213 \\ 0.0900 \\ 0.0622 \\ 0.0000 \\ 0.0026 \\ 0.0324 \\ 0.0125 \\ 0.0649 \\ 0.0682 \\ 0.0150 \\ 0.0014 \\ 0.0664 \\ 0.0371 \\ 0.1163 \\ 0.0159 \\ 0.0218 \\ 0.0278 \\ 0.0000 \\ 0.0092 \\ 0.0000 \end{pmatrix} \quad f' = \begin{pmatrix} 0.0889 \\ 0.0122 \\ 0.0270 \\ 0.0505 \\ 0.1437 \\ 0.0226 \\ 0.0244 \\ 0.0697 \\ 0.0592 \\ 0.0000 \\ 0.0026 \\ 0.0366 \\ 0.0113 \\ 0.0671 \\ 0.0810 \\ 0.0131 \\ 0.0009 \\ 0.0688 \\ 0.0383 \\ 0.1098 \\ 0.0183 \\ 0.0209 \\ 0.0244 \\ 0.0000 \\ 0.0087 \\ 0.0000 \end{pmatrix}$$

Slika 3. 3 Usporedba frekvencija prvih lijevih i desnih singularnih vektora s vektorom frekvencija $\boldsymbol{f}$

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

3.3 Kriptoanaliza Hillove šifre

Hillova šifra je vrsta polialfabetske 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 **x** dimenzija *n*. Šifrirani vektor $\boldsymbol{y_i}$ dobiva se modulo *l* množenjem ključa *K*, predstavljen nesingularnom matricom *n* x *n*, vektorom $\boldsymbol{x_i}$. Odnosno,

$$\boldsymbol{y_i} = K\boldsymbol{x_i}\ (mod\ l). \tag{3-10}$$

Šifrirana *n* x *n* matrica *Y* (*n* stupaca matrice su zapravo *n*-dimenzionalni vektori $\boldsymbol{y_i}$) se po istom principu dobiva produktom ključa i matrice otvorenog teksta *X (n* stupaca matrice su zapravo *n*-dimenzionalni vektori $\boldsymbol{x_i}$) i vrijedi

$$Y = KX\ (mod\ l). \tag{3-11}$$

Postupak dešifriranja je razumljivo tada

$$\boldsymbol{x_i} = K^{-1}\boldsymbol{y_i}\ (mod\ l), \tag{3-12}$$

odnosno za slučaj s matricama

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

Problem s kojim se susreće kriptoanalitičar 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 **x** i dio šifrata, odnosno šifriranih vektora $\boldsymbol{y}$. Postoji mogućnost formiranja invertibilne matrice *n* x *n (mod l)* uz poznavanje samo dijela otvorenog teksta. Tada se $K\boldsymbol{x_i} = \boldsymbol{y_i}$ može zapisati u obliku $K = \boldsymbol{y_i}\boldsymbol{x_i}^{-1}$ odakle se dobiva šifrerska 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 kriptoanalitičar 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 $\boldsymbol{x_i}$ i $\boldsymbol{y_i}$, a time ni određivanje matrica 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 ZSHLFGLKTVDUWAQBCG 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:

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

Zadaća je konstruirati 2 x 2 matricu invetribilnu 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 $det(M)=-295\equiv 17\ (mod\ 26)$. 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.

$$\boldsymbol{y_i}=K\boldsymbol{x_i}=\begin{bmatrix}11&17\\18&2\end{bmatrix}\begin{bmatrix}2\\17\end{bmatrix},\begin{bmatrix}24\\15\end{bmatrix},\begin{bmatrix}19\\14\end{bmatrix},\begin{bmatrix}6\\17\end{bmatrix},\begin{bmatrix}0\\15\end{bmatrix},\begin{bmatrix}7\\24\end{bmatrix},\begin{bmatrix}8\\18\end{bmatrix},\begin{bmatrix}2\\14\end{bmatrix},\begin{bmatrix}14\\11\end{bmatrix}$$

$$=\begin{bmatrix}25\\18\end{bmatrix},\begin{bmatrix}25\\20\end{bmatrix},\begin{bmatrix}5\\6\end{bmatrix},\begin{bmatrix}17\\12\end{bmatrix},\begin{bmatrix}21\\4\end{bmatrix},\begin{bmatrix}17\\18\end{bmatrix},\begin{bmatrix}4\\24\end{bmatrix},\begin{bmatrix}0\\12\end{bmatrix},\begin{bmatrix}3\\14\end{bmatrix}.$$

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 kriptoanalitičar 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* x *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* , $det(M) = -791 \equiv 15\ (mod\ 26)$, 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 potrvđuje 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:

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

Pošiljatelj tada računa sljedeću vrijednost:

$$h \equiv f^{-1}\, g \;(mod\; q), \qquad 0 < h < q. \tag{3-14}$$

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

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

Šifrat se dobiva izračunom

$$e = rh + m \;(mod\; q), \qquad 0 < e < q. \tag{3-15}$$

Primalac dobiva šifrat i najprije određuje

$$a \equiv fe \;(mod\; q), \qquad 0 < a < q \tag{3-16}$$

i nakon toga otvoreni tekst dobiva iz

$$b \equiv f^{-1}a \;(mod\; g), \qquad 0 < b < g. \tag{3-17}$$

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:

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

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 $a \equiv fe \;(mod\; q)$ uz $0 < a < q$, dobiva točno određenu vrijednost

$$a = rg + fm \tag{3-18}$$

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

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

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

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

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

$$f^{-1} \equiv 49194372303 \,(mod\ q) \quad i \quad h \equiv f^{-1}g \equiv 39245579300 \,(mod\ q).$$

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:

$$e \equiv rh + m \equiv 18357558717 \,(mod\ q).$$

Primalac dekriptira poruku korištenjem svojeg privatnog ključac f. Najprije računa

$$a \equiv fe \equiv 48314309316 \,(mod\ q).$$

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

$$f^{-1}a \equiv 193495 \cdot 48314309316 \equiv 123456 \,(mod\ g).$$

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 kriptoanalitičara pronalazak bilo kojeg para brojeva $F, G \in \mathbb{N}$ koji zadovoljava:

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

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

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

Problem je sada sveden na traženje linearne kombinacije $\boldsymbol{w} = a_1\boldsymbol{v_1} + a_2\boldsymbol{v_2}$ na temelju poznatih vektora $\boldsymbol{v_1} = (1, h)$ i $\boldsymbol{v_2} = (0, q)$ duljine $\mathcal{O}(q)$ te poznate duljine vektora $|\boldsymbol{w}| = \mathcal{O}(\sqrt{q})$, koeficijenti a_1 i a_2 su cijeli brojevi. Prema tome kriptoanalitičar mora pronaći vektor kojemu je modul mali broj različit od nule i pripada skupu vektora

$$L = \{a_1\boldsymbol{v_1} + a_2\boldsymbol{v_2} : \ a_1, a_1 \in \mathbb{Z}\}.$$

Skup L je primjer jedne dvodimenzionalne mrežaste strukture. U suštini dvodimenzionalni vektorski prostor s bazom $(\boldsymbol{v_1}, \boldsymbol{v_2})$ 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),

$$\boldsymbol{v_1} = (1, 39245579300) \quad i \quad \boldsymbol{v_2} = (0, 122430513841).$$

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

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

Uz zanemarivanje predznaka, kriptoanalitičar 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 Massachusets,* 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 matričnih sustava, vektora i njihovih svojstava lako se implementiraju na računalima.

Summary

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

As modern communication's are mostly digital, processed via computer, thus cryptography and algorithms has 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