Universiteti i Prishtinës “Hasan Prishtina”

Fakullteti i Shkencave Matematiko – Natyrore

Programi: Shkenca Kompjuterike

Lënda: Siguria e të dhënave

Tema: Algoritmi i Hill Cipher

Punoi:

Egzonit Demhasaj

Gabriel Kolaj

Profesorët:

Artan Berisha

Besnik Duriqi

Algoritmi Hill Cipher

Hill Cipher është një shifrim poligrafik me zëvendësim i bazuar në algjeber lineare. Ky shifrim është krijuar nga Lester S. Hill ne vitin 1929. Qe Hilli të mos akuzoj se sistemi i tij të mos jetë tepër i komplikuar për përdorim të përditshem, ai krijoi një makine shifruese duke përdorur një seri prej rrotave dhe zingjirë të pajisur. Kontributi i Hill'it ka qene në menyrën sesi e ka perdorur matematikën për të dizajnuar por edhe krijuar kriptosisteme. Një gjë qe duhet ditur është se për analizimin e algoritmeve duhet të studiohët një degë e matematikës e njohur si teoria e numrave. Secila shkronjë është e reprezentuar nga një numer modulo 26. Pra, për A = 0, B = 1, ..., Z = 25. Qe të enkriptohët një mesazh, secili bllok p përbërë nga *n* shkronja shumezohët me një matricë të perkëmbyeshme *n x n*, sipas modulo 26. Qe të enkriptohët mesazhi, secili bllok shumezohët me matricën inverse qe është përdorur për enkriptim. Matrica e përdorur për çeles shifrimi duhet të merret e rastësishme dhe të jetë e përkembyeshme nga bashkesia e matricave *n x n* të përkembyeshme modulo 26. Qka duhet pasur parasysh është rritja e kompleksitetit me rritjen e çelsit të matrices.

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
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

Fig.1. Tabelja e shkronjave qe i korrospondon numrave përkatse tek Shifrimi Hill

Enkriptimi përmes Hill Cipher

Qe të enkriptojmë një tekst duke përdorur Hill Cipher, ne duhët të kryejmë operacionet si ne vijim.

$$E(K, P) = (K * P)\ mod\ 26$$

Ku *K* paraqet çelsin e matrices dhe *P* është teksti në formën vektoriale. Shumezimi i ketyre dy matricave gjeneron tekstin e enkriptuar. Nese teksti i cili deshirojmë ta enkriptojmë ka me shumë së gjatesinë 3 atëherë teksti duhet ndarë qdo 3 shkronja, në rastin e mbetjes së disa blloqe pa mbushur (zakonisht ne fund) shtojmë disa shkronja të rastësishme qe të permbushin bllokun. **Shembull.** Fjala "*ATTACK ON DAWN*" mund të ndahët si 'ATT', 'ACT', 'OND','AWN'.

Shembulli

Supozojme së kemi një tekst qe dojme ta enkriptojmë, në rastin tone tekstin 'HEY' (ku n = 3). Çelsin e marrim 'GYBNQKURP' e cila mund të shkruhët ne matricë si:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Dhe mesazhin ‘HEY’ si:

$$\begin{bmatrix} 7 \\ 4 \\ 24 \end{bmatrix}$$

Ku vektori i shifruar është dhënë nga:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \\ 24 \end{bmatrix} = \begin{bmatrix} 162 \\ 395 \\ 568 \end{bmatrix} = \begin{bmatrix} 162 \\ 395 \\ 568 \end{bmatrix} (mod\ 26)$$

Qe në rastin e enkriptimit teksti ‘HEY’ shëndërrohet ne ‘GFW’, ku ne vijim është paraqitur matrica pas operimeve modulo:

$$\begin{bmatrix} 6 \\ 5 \\ 22 \end{bmatrix}$$

Dekriptimi përmes Hill Cipher

Mënyra sesi të dekriptojmë kodin e shifruar në vektor përseri është vetem me shumezimin e matricës inverse të çelsit, pra si në vijim:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} (mod\ 26) \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

Duke rikujtuar se në enkriptim morem tekstin ‘GFW’, tani me dekriptim marrim:

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 162 \\ 395 \\ 568 \end{bmatrix} = \begin{bmatrix} 8951 \\ 18490 \\ 12686 \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \\ 24 \end{bmatrix} (mod\ 26)$$

Qe na dergon përseri tek teksti i mëparshem apo ‘HEY’.

Por ekzistojnë dy probleme me përzgjedhjen e matricës se enkriptuar:

1) Jo të gjitha matricat kane një inversë. (Nje matric ka inverse atëherë dhe vetem atëherë nese determinanta e saj nuk është e barabartë me 0).
2) Determinanta e matricës se enkriptuar duhet të mos ketë faktor të përbashket me modulon (mod 26 perkatesisht).

Por faktori i 2) mund të eliminohet duke bërë modulon një numer të thjeshtë.

Siguria dhe atvantazhet

Disa nga atvantazhët e Hill Cipher jane:

1) Se fsheh në menyrë përfekte frekuencat me një shkronjë.
2) Shifrimi Hill është shumë efektive për të fshehur informatat me një apo dy letra me frekuencë
3) Është shumë i forte ndaj sulmeve me tekst shifrues, por i dobët ndaj atyre qe janë me tekst të thjeshtë.

Hill Cipher është i dobet ndaj sulmeve "*known – plaintext attack*" meqense është plotësisht linear. Nese ndonjë keqbërës përcepton n^2 text të shifruar karakteret e çifteve mund të formojnë një sistem linear i cili shume lehtë mund të zgjidhet, nese kjo ndodh atëherë mund të shtohën vetem edhe disa çifte dhe sistemi merr vetem pak kohe dhe mund të zgjidhet. Teksti i shifruar në Hill Cipher nuk mund të jepë ndoshta siguri në ditet e sodit, por me kombinimin e matricave tjera jo – lineare matrica mund të jetë e dobishme ne operacione tjera si "S – boxes". Nje shembull qe mund të marrim është rasti i shifrimit Hill në një matrice 2 x 2 ku ne mund të sulmojmë duke matur frekuencat e secilit diagraf qe ndodhët ne tekstin e shifruar. Ne gjuhe angleze diagrafi me së shpeshti qe përdoret është 'th', pas tij vjen 'he'. Nese në e dijm qe Hill Cipher është përdorur dhe diagrafi me së shumti i përdorur është 'kx', pas tij menjëherë 'vz' (shembull), ne mund të supozojme se 'kx' dhe 'vz' korrospondojnë me 'th' dhe 'he', respektivisht. Kjo do të thotë qe [19, 7] dhe [7, 4] jane të derguar tek [10, 23] dhe [21, 25] respektivisht.

Madhesia e bashkesise së çelsave – Bashkesia e çelsave paraqet një varg te çelsave të mundshem, ndërsa madhesia e bashkesisë se çelsave paraqet numrin e çelsave të mundshem. Kto shkruhen në numra binare dhe mund të llogaritën me logaritmin binar të madhesise se çelsave.

Konkluzioni

Hill Cipher është njëri ndër sistemet e shifrimit poligrafik paresore të ndertuara ne sisteme praktike i cili përdor me shumë se 3 simbole apo shkronja ne një. Në kohen modernë Hill Cipher thuajse nuk përdoret fare, por ekzistenca e saj është një mesim i mirë drejt hapave të parë të kuptimit të kriptografisë. Një matrice 2 x 2 të shifrimit Hill mund të zgjidhet dhe dekriptohet shumë lehtë, por me rastin e rritjes së saj në madhesi kalkulimet bëhen shumë me të veshtira dhe kerkojne një kuptim me të thelle të matematikës se lartë në thellësi.

Referencat

[1] https://en.wikipedia.org/wiki/Hill_cipher

[2] https://www.javatpoint.com/hill-cipher-program-in-java

[3] https://www.geeksforgeeks.org/hill-cipher/

[4] Practical Cryptography