UNIVERSITETI I PRISHTINES FAKULTETI I SHKENCAVE MATEMATIKO-NATYRORE

Tema: Zhvendosja e shifrës (ose shifra e Cezarit)

Lënda: Siguria e të Dhënave

Punuar nga:

Ardit Maliqi
Atlant Klaiqi
Andi Alidema

Ligjëruesit e lëndës:

Prof.Artan Berisha
Ass.Besnik Duriqi

Historiku i Zhvendosjes me shifër (shifra e Cezarit) :

Zhvendosja e Shifrës është një nga metodat më të vjetra dhe më të thjeshta të enkriptimit, që daton që në kohët e lashta. Është një lloj shifrmi zëvendësues ku çdo shkronjë në tekstin e thjeshtë zhvendoset në një numër të caktuar vendesh poshtë alfabetit.

Zhvendosja e shifrës, e njohur gjithashtu si Shifra e Cezarit, është emëruar pas Julius Ceasar, i cili thuhet se ka përdorur këtë teknikë të enkriptimit për të komunikuar me gjeneralët e tij, për të dhënur urdhërat e tij që nëse duhet të sulmojnë apo jo. Shifra e Cezarit është një nga teknikat më të thjeshta dhe më të vjetra të enkriptimit, që daton nga Perandoria Romake.

Shifra e Cezarit besohet të jetë përshkruar për herë të parë nga histroiani romak Suetonius, i cili shkroi se Jul Cezari përdori një zëvendësim të thjeshtë të shkronjave për të koduar mesazhet e tij. Në këtë teknikë të enkriptimit, çdo shkronjë në tekstin e thjeshtë zëvendësohet me një shkronjë një numër fiks pozicionesh poshtë alfabetit. Cezari përdori një vlerë ndryshimi prej 3, kështu që çdo shkronjë në tekstin e tij të thjeshtë u zëvendësua me shkronjën tre pozicione pas asaj në alfabet.

Shifra e Cezarit nuk u përdor gjerësisht gjatë kohës së Cezarit, por u bë më e popullarizuar gjatë Mesjetës. Kjo metodë u përdor nga murgjit për të kriptuar tekste fetare dhe dokumente të tjera, dhe u përdor gjithashtu nga udhëheqës ushtarakë dhe politikë për të komunikuar informacione të ndjeshme.

Megjithë thjeshtësinë e tij, Shifra e Cezarit mbeti teknikë e njohur e enkriptimit për shekuj, derisa u zhvilluan metoda më të avancuara të kriptimit në epokën moderne. Shifra e Cezarit përdoret herë pas here edhe sot, kryesisht për qëllime edukative ose si pjesë e algoritmeve më komplekse të enkriptimit.

Shifra e Cezarit ka luajtur një rolë të rëndësishëm në zhvillimin e kriptografisë, duke shërbyer si bazë për teknikat më të avancuara të enkriptimit. Mbetet një pjesë e rëndësishme e historisë së kriptografisë dhe ende studiohet dhe analizohet nga studiuesit sot.

Në shekullin e 19-të, shifra e ndërrimit përdorej shpesh në telegrafi, ku ishte e nevojshme që mesazhet të enkripoheshin shpejt dhe me efikasitet. Gjatë Luftës së Parë Botërore dhe Luftës së Dytë Botërore, shifra e ndërrimit u përdor gjerësisht nga forcat ushtarake, por përfundimisht u zëvendësua nga metoda më të sofistikuara të enkriptimit si makina Enigma.

Si funksionon në mënyrë matematikore zhvendosja e shifrave

Zhvendosja shifrore është një shifër e thjeshtë zëvendësuese që përshfin zhvendosjen e shkronjave në një mesazh me një numër të caktuar pozicionesh poshtë alfabetit. Për të kryer enkriptimin, fillojmë me një mesazh teksti të thjeshtë dhe një çelës që specifikon numrin e pozicioneve për të zhvendosur secilën shkronjë.

Për të performuar këtë enkriptim, ne mund të paraqesim çdo shkronjë në mesazhin me tekst të thjeshtë si një numër, ku A është 0, B është 1, e kështu më radhë, deri në Z është 25. Më pas aplikojmë zhvendojsen duke shtuar çelësin në numrat e secilës shkronjë përfaqësimi dhe duke marrë modulin e rezultatit 26 për t'u siguruar që qëndrojnë brenda intervalit 0 deri në 25. Për shembull, nëse mesazhi me tekst të thjeshtë është "HELLO" çelësi është 3, do të merrnim:

H	$e_3(7) = (7 + 3)\ mod\ 26 = 10\ mod\ 26$	K
E	$e_3(4) = (4 + 3)\ mod\ 26 = 10\ mod\ 26$	H
L	$e_3(11) = (11 + 3)\ mod\ 26 = 14\ mod\ 26$	O
L	$e_3(11) = (11 + 3)\ mod\ 26 = 14\ mod\ 26$	O
O	$e_3(14) = (14 + 3)\ mod\ 26 = 17\ mod\ 26$	R

Ku mesazhi i enkripuar do të jetë "KHOOR". Po ashtu pas dekriptimit të fjalës "KHOOR" do të kthehej përsëri fjala "HELLO".

Formula e përgjithshme për Zhvendosjen e shifrave:

Le të jetë x, y, k $\in Z_{26}$

Enkriptimi	$e_k(x) \equiv (x + k)\ mod\ 26$
Dekriptimi	$d_k(y) \equiv (y - k)\ mod\ 26$

Mënyrat e sulmimit të Zhvendosjes me shifër (Shift cipher)

- ➢ Sulmi me brute force: Sulmi me brute force është mënyra më e thjeshtë për të sulmuar cipherin e ndryshimit. Kjo përfshin provimin e çdo kombinimi të mundshëm derisa plaintexti të gjendet. Meqenëse ka vetëm 26 shkronja të mundshme, dmth është një metodë e arritshme. Megjithatë, kërkon kohë dhe kërkon fuqi kompjuterike të konsiderueshme.
- ➢ Analiza e frekuencës: Një tjetër mënyrë për të sulmuar cipherin e ndryshimit është përdorimi i analizës së frekuencës. Kjo përfshin analizën e frekuencës së shkronjave në ciphertext. Në një tekst, disa shkronja përdoren më shpesh se të tjerët. Për shembull, shkronja 'e' është shkronja më e përdorur në gjuhën angleze. Duke analizuar frekuencën e shkronjave në ciphertext, një person mund të bëjë parashikime rreth ndryshimit të përdorur dhe të provojë të dekriptojë mesazhin.
- ➢ Sulmi i plaintextit të njohur: Për të kryer një sulm të tillë duhet pasur një dije të caktuar për plaintextin. Ky mund të jetë një fjalë ose frazë që dihet se është e pranishme në mesazh. Duke përdorur këtë dijeni, një person mund të provojë të kuptojë ndryshimin e përdorur dhe të dekriptojë pjesën tjetër të mesazhit.
- ➢ Sulmi i fjalorit: Një sulm i fjalorit përfshinë përdorimin e një liste të njohur të fjalëve për të provuar dekriptimin e mesazhit.Kjo metodë është më efikase se brute force attack sepse e redukton numrin e përgjithshëm të rasteve që duhen provuar.
- ➢ Kriptoanaliza: Kriptoanaliza është një teknikë më e avancuar e përdorur për të sulmuar zhvendosjen e shifrës. Ai e përfshin analizimin e strukturës së metodës së enkriptimit dhe gjetjen e dobësive në algoritëm. Duke përdorur kriptoanalizën, një person mund të thyejë shifrën pa provuar të gjitha ndërrimet e mundshme.

Algoritmi i Zhvendosja e shifrave për enkriptim:

1. Vendosni vlerën e zhvendosjes, që është numri i pozicioneve që çdo shkronjë zhvendoset poshtë alfabetit.
2. Krijo dy vargje, një për mesazhin origjinal dhe një për mesazhin e koduar.
3. Për çdo karakterë në mesazhin origjinal:
   3.1. Nëse karakteri është një shkronjë, ktheje atë në numrin përkatës në alfabet (A=0, B=1, …. , Z=25).
   3.2. Zhvendosni numrin poshtë alfabetit me vlerën e zhvendosjes.

3.3. Nëse numri i zhvendosur është më i vogël se 0, shtoni 26 (numrin e shkronjave në alfabet) për ta mbështjellë në fund të alfabetit.
3.4. Nëse numri i zhvendosur është më i madh ose i barabartë me 26, zbritni 26 për ta mbështjellë në fillim të alfabetit.
3.5. Kthejeni numrin e zhvendosur përsëri në shkronjën e tij përkatëse.
3.6. Shtoni letrën në vargun e mesazheve të koduara.
3.7. Nëse karakteri nuk është një shkronjë shtojeni atë në vargun e mesazhit të koduar siç është.

4. Ktheni vargun e mesazhit të koduar.

Algoritmi në java per Zhvendoesjen e shifrës:

```
public static StringBuffer encrypt(String text, int s)
    {
        StringBuffer result= neë StringBuffer();

        for (int i=0; i<text.length(); i++)
        {
            if (Character.isUpperCase(text.charAt(i)))
            {
                char ch = (char)(((int)text.charAt(i) +
                                  s - 65) % 26 + 65);
                result.append(ch);
            }
            else
            {
                char ch = (char)(((int)text.charAt(i) +
                                  s - 97) % 26 + 97);
                result.append(ch);
            }
        }
        return result;
    }
```