UNIVERSITETI I PRISHTINËS "HASAN PRISHTINA"
FAKULTETI I SHKENCAVE MATEMATIKO-NATYRORE
DEPARTAMENTI I MATEMATIKËS
PROGRAMI: SHKENCA KOMPJUTERIKE

Lënda: Siguria e të dhënave
Algoritmi Affine Cypher

Punuar nga:

1. **Rinesë Morina**
2. **Rona Latifaj**
3. **Eljesa Kqiku**

Mars 2023

Përshkrimi

Shifra Affine është një lloj shifrimi me zëvendësim ku çdo shkronjë në tekstin e thjeshtë zhvendoset për disa pozicione. Është një shifër monoalfabetike, që do të thotë se çdo shkronjë zëvendësohet me të njëjtën shkronjë gjatë gjithë mesazhit. Megjithatë, ndryshe nga Shifra e Cezarit, Shifra Affine përdor një formulë matematikore pak më komplekse për të kriptuar mesazhin.

Për të enkriptuar një mesazh duke përdorur shifrën Affine, zgjidhen dy numra, a dhe b. Shkronjat e tekstit të thjeshtë përfaqësohen më pas me numra sipas pozicionit të tyre në alfabet

$$A = 0, B = 1, C = 2, ...$$

dhe më pas transformohen duke përdorur formulën e mëposhtme:

$$C = (a * P + b) mod 26$$

ku C është shkronja e tekstit të shifruar, P është shkronja e tekstit të thjeshtë (e përfaqësuar nga një numër) dhe mod 26 do të thotë që rezultati është marrë moduli 26 (d.m.th., pjesa e mbetur kur ndahet me 26).

Për të deshifruar tekstin e shifruar, përdoret formula e mëposhtme:

$$P = a^{-1} * (C - b) mod 26$$

ku a^{-1} është inversi multiplikativ modular i a (d.m.th., numri që, kur shumëzohet me a, jep rezultatin 1 modulo 26).

Historia

Shifra Affine është një nga llojet më të vjetra të metodave të kriptimit, që daton që nga qytetërimet e lashta si grekët dhe romakët. Në fakt, vetë Julius Cezari thuhet se ka përdorur një version të thjeshtë të Affine Cipher për t'u dërguar mesazhe gjeneralëve të tij gjatë fushatave. Megjithatë, formula matematikore e përdorur në versionin modern të Affine Cipher nuk u zhvillua deri në shekullin e 15-të, kur matematikani italian Leon Battista Alberti krijoi një shifër polialfabetike që bazohej në një formulë të ngjashme.

Raste të përdorimit

Affine Cipher është një metodë relativisht e thjeshtë enkriptimi që mund të përdoret në një sërë situatash ku kërkohet një nivel bazë sigurie. Disa raste të përdorimit të zakonshëm përfshijnë:

- Enkriptimi i mesazheve ndërmjet dy palëve që kanë rënë dakord për vlerat e a dhe b
- Kriptimi i fjalëkalimeve ose të dhënave të tjera të ndjeshme që nuk kërkojnë siguri të nivelit të lartë
- Demonstrimi i parimeve bazë kriptografike në mjediset arsimore

Algoritmi formal

Enkriptimi

HYRJA: Numrat a dhe b që formojnë çelësin (a, b), gjatësia e mesazhit n, vargu i karakterëve të mesazhit origjinal P=p_i, ku $1 \leq i \leq n$
DALJA: Vargu i karakterëve të enkriptuar C=c_i, ku $1 \leq i \leq n$
HAPI 1: Për çdo $i = 1, 2, ..., n$ ekzekuto Hapin 2
HAPI 2: Nese $p_i =$ " " atehere:
$c_i =$ " ";
Përndryshe
$c_i = (a * p_1 + b) mod 26$;
HAPI 3: Kthe(C=c_i $1 \leq i \leq n$); Ndalo;

Dekriptimi

HYRJA: Numrat a dhe b që formojnë çelësin (a, b), gjatësia e mesazhit n, vargu i karakterëve të mesazhit të enkriptuar C=c_i, ku $1 \leq i \leq n$
DALJA: Vargu i karakterëve të dekriptuar P=p_i, ku $1 \leq i \leq n$
HAPI 1: Për çdo $i = 1, 2, ..., n$ ekzekuto Hapin 2
HAPI 2: Nese $c_i =$ " " atehere:
$p_i =$ " ";
Përndryshe
$p_i = a^{-1} * (c_i - b) mod 26$;
HAPI 3: Kthe(P=p_i $1 \leq i \leq n$); Ndalo;

Shembull

Supozoni se duam të enkriptojmë mesazhin "HELLO" duke përdorur kodin Affine me $a = 5$ dhe $b = 8$. Së pari, ne përfaqësojmë çdo shkronjë si një numër sipas pozicionit të saj në alfabet:

H	E	L	L	O
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
7	4	11	11	14

Më pas, aplikojmë formulën e enkriptimit për secilën shkronjë:

$$C(H) = (5 * 7 + 8) mod 26 = 11 = L$$
$$C(E) = (5 * 4 + 8) mod 26 = 22 = W$$
$$C(L) = (5 * 11 + 8) mod 26 = 9 = J$$
$$C(L) = (5 * 11 + 8) mod 26 = 9 = J$$
$$C(O) = (5 * 14 + 8) mod 26 = 12 = M$$

Prandaj, mesazhi i koduar është "$LWJJM$". Për të deshifruar mesazhin, përdorim formulën e deshifrimit me a^{-1}=21 (pasi 5*21 $\equiv$ 1 mod 26):

$$P(L) = (21 * (11 - 8)) mod 26 = 7 = H$$
$$P(W) = (21 * (22 - 8)) mod 26 = 4 = E$$
$$P(J) = (21 * (9 - 8)) mod 26 = 11 = L$$
$$P(J) = (21 * (9 - 8)) mod 26 = 11 = L$$
$$P(M) = (21 * (12 - 8)) mod 26 = 14 = O$$

Prandaj, mesazhi i deshifruar është "$HELLO$"

Në këtë shembull, ne kemi përdorur $a = 5$ dhe $b = 8$ si çelësat e enkriptimit. Sidoqoftë, çdo vlerë e a dhe b mund të përdoret për sa kohë që ekziston inversi multiplikativ i a modulo 26. (pra a dhe 26 janë relativisht të thjeshtë).

Sa më të mëdha të jenë vlerat e a dhe b, aq më i sigurt do të jetë kriptimi, por edhe aq më i vështirë do të jetë deshifrimi pa i ditur çelësat. Në përgjithësi, Affine Cipher është një metodë e thjeshtë por efektive e kriptimit që është përdorur për shekuj. Ndonëse mund të mos jetë aq i sigurt sa algoritmet moderne kriptografike, mund të jetë ende i dobishëm në situata të caktuara ku kërkohet kriptimi bazë.

Implementimi në Java

```
public class AffineCypher {
    static int a = 17;
    static int b = 20;

    static String encryptMessage(char[] msg)
    {

        String cipher = "";
        for (int i = 0; i < msg.length; i++) {
            if (msg[i] != ' ')
                cipher = cipher
                        + (char) ((((a * (msg[i] - 'A')) + b) % 26) + 'A');
            else
                cipher += msg[i];
        }
        return cipher;
    }

    static String decryptCipher(String cipher)
    {
        String msg = "";
        int a_inv = 0;
        int flag = 0;

        for (int i = 0; i < 26; i++) {
            flag = (a * i) % 26;
            if (flag == 1)
                a_inv = i;
        }
        for (int i = 0; i < cipher.length(); i++) {
            if (cipher.charAt(i) != ' ')
                msg = msg + (char) (((a_inv *
                        ((cipher.charAt(i) + 'A' - b)) % 26)) + 'A');
            else
                msg += cipher.charAt(i);
        }
```

```
37          return msg;
38      }
39  }
```