المحاضرة السابعة:

3. Multiplicative Cipher: الشفرة الضربية

تخضع هذه العملية Substitution Multiplicative Cipher للقانون التالي:

$$C = E_k(p) = (p*k) \bmod 26$$

$$C = p*k$$

ملاحظة: يجب تحقق الشرط التالي في الخوارزمية وهو ان كلا العددين k و26 يقبل القسمة على نفسه والواحد أي العلاقة التي تربط المفتاح k مع الرقم 26 هو عدد اولي أي القاسم المشترك بينهما هو 1.

The Condition to key is k and 26 relatively prime

$$GCD(26 , k) = 1$$

القاسم المشترك الأعظم GCD: هو اكبر عدد مشترك بين الرقمين

ملاحظة: المفتاح المستخدم في هذه الطريقة يجب ان يطابق الشرط التالي

$$GCD = gcd(k , 26)=1$$

أي ان المفتاح يشمل جميع القيم الفردية المحصورة بين 0 و 25 ماعدا الرقم 13 لأنه لا يحقق الشرط السابق. نلاحظ ان:

$GCD(26 , 2) = 2 \Longrightarrow k=2$ غير مقبول

$GCD(26 ,3) = 1 \Longrightarrow k=3$ مقبول

$GCD(26 , 13) = 13 \Longrightarrow k=13$ غير مقبول

الأرقام المقبولة كمفتاح $k=\{1,3,5,7,9,11,15,17,19,21,23,25\}$

$$C = P * k$$

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
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

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

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

Let h=3

C_1= 1*3 = 3 = C

C_2 =2*3=6 =F

C_3 = 3*3 = 9 =I

C_{10} = 10*3 = 30 $\Longrightarrow$ 30/26 =1 mod $\Longrightarrow$ 4 =D

ملاحظة: السبب في عدم أخذ الأعداد الزوجية ورقم 13 في المفتاح key هو أن الأحرف سوف تتكرر في النص المشفر وهنا يصبح لدينا خطأ في التشفير ومشكلة في فك الشفرة

Acceptable Alphabet **الهجائيات المقبولة**

تحوي كل الحروف المطلوبة المستخدمة بدون تكرار

Example: Let the plan text (**GOOD**), Where k=3, Find cipher text using multiplicative cipher

الحل

G o o d

7 15 15 4 $\Longleftarrow$ تسلسل الاحرف الابجدي

نشفر

C=P*K

C_1 = 7 * 3 =21` =U

$C_2 = 15 * 3 = 45 \longrightarrow 45 \bmod 26 \ldots\ldots > \text{mod}45/26 = 19$ الباقي $= S$

$C_3 = 4*3 = 12 = L$

Plain: G O O D

Cipher: U S S L المشفر

ملاحظة: في عملية (الاضافة) Addition تكون جميع المفاتيح مقبولة

$C=p+k$

اما في عملية الضرب Multiplicative فتكون بعض النتائج مقبولة والأخرى غير مقبولة

$C=p*k$

Example: If P =GOOD, k =2. Find cipher text using Multiplication

Cipher method Multiplicative فك الشفرة

$p = (c / k) \bmod 26$

---

4. Affine Substitution Cipher:

هذه الطريقة تجمع بين الطريقتين (direct +Multiplicative):

وتخضع للقانون الآتي:

$$C=E_{k1,k2}(m) = (m * k_1 + k_2) \bmod 26$$

اذن القانون ببساطة لهذه الطريقة هو:

$$C = m * k_1 + k_2$$

Example: Encrypt plain text { computer } by using Affine cipher ?

with key [3, 5]

3 15 13 16 21 20 5 18

C o m p u t e r

C_1 = 3* 3+5 =14= N

C_2 = 15 * 3 + 5 =24=X

C_3= 13 * 3+5 =18=R

C_4=16 *3 +5 =11= A

C_5=21*3+5=16=P

C_6=20*3+5=13=M

C_7= 5*3+5=20=T

C_8=18*3+5=7=G

Cipher text =NXRAPMTG

لفك شفرة طريقة Affine لدينا القانون التالي:

m= ((c-k2)÷k1) mod 26

Or p=(c-k2)/k1

H.W.: Encrypt the following words by using Affine cipher

1- Iraq; 2- University; 3- human; 4- Good morning

5- Mixed alphabet substitution