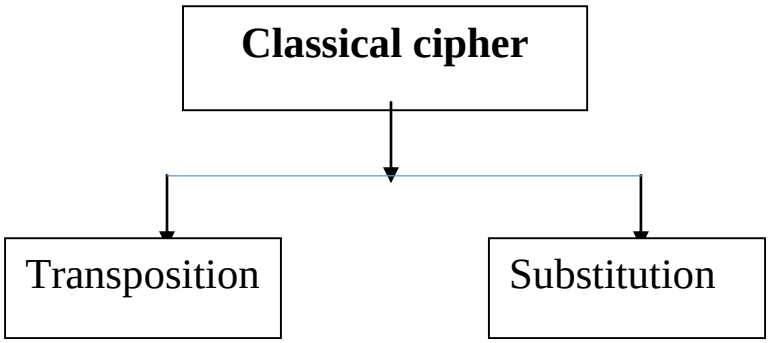
المحاضرة السادسة:



Substitution ciphers: **الشفرات التعويضية**

In general, replace the character of message with another one.

1- Direct standard (Caesar Cipher) شفرة قيصر او الشفرة المباشرة

2- Reciprocal (Reversal) Cipher الشفرة العكسية

3-Multiplicative Cipher الشفرة الضربية

4- Affine Cipher (Direct+ Multiplicative) شفرة افين

5- Mixed alphabet مزج الهجائيات

6- Key word Mixed (Key phrase) مزج الكلمة المفتاحية

7-Transposed keyword Mixed مزج الكلمة المفتاحية الابدالية

1- Direct standard (Addition Cipher)

Plain text ازاحة الهجائية بثلاث مراتب لـ

Alphabet of plain الاحرف الهجائية للنص

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

مثال: باستخدام الطريقة المباشرة direct أو Caesar شفر كلمة computer؟

Plain Text: C O M P U T E R

Cipher Text: F R P S X W H U

إذا معادلة Caesar Cipher تكون كالآتي:

$$C=E_K(m) = (m+K) \bmod 26$$

modulo addition (الجمع المعياري)

إذ أن k: تمثل مقدار الإزاحة no. of shift

اذا يتم عمل الـ mod حسب طول الأحرف الهجائية، لذا يجب ان يكون الناتج يقع بين او ضمن ال mod.

مثال :- اذا كان ال mod =26

اذن الناتج يقع بين 25 ⟵ 0

على سبيل المثال:

13 +17=30 جمع عادي

13+17 =4 جمع معياري

الجمع المعياري ينتج من قسمة الرقم الناتج من الجمع العادي على 26 واخذ الباقي الذي يمثل الجمع المعياري

مثال: في شفرة قيصر مقدار الازاحة k=3

Computer

$C_1=m+k$

$C_1 = 3+3 = 6 = F$

C ⟵ F اذن

C2= 15+3 = 18 = R

O ⟶ R

وهكذا

Plain text: C O M P U T E R

Cipher text: F R P S X W H U

عندما K=7

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

H I J K L M N O P Q R S T U V W X Y Z A B C D E F G

مثال: قم بتشفير الكلمة Security باستخدام شفرة قيصر عندما k=7

P: Security

c1=19+7=26 = ...=z

s ⟶ z

c2= 5 +7=12=L ⟹ e ⟶ L

K=7 بازاحة

P: S E C U R I T Y

C : Z L J B Y P A F

اذن

مقدار الازاحة أو الرقم الذي سوف نضيفه K={0,1,2,3.....,25}

Decryption فك التشفير بهذه الطريقة :

معادلة فك الشفرة **M=(C-K) MOD 26**

ملاحظة : دائما نعمل اضافة 26 الى الرقم اذا كان سالب

ملاحظة بمعنى أنه اذا كان لدينا المشفر k عندئذ نستطيع استخراج الحرف الأصلي من مقدار الازاحة.

مثال : أعد النص المشفر cipher text : Z L J B YP A F الى النص الصريح؟

ما هي قيمة الحرف الصريح m اذا علمت ان k =7 , cipher =26=z

الحل:- حسب قانون معدل فك الشفرة كالآتي:

m=26-7 =19 =s

S موقعها بتسلسل الاحرف الابجدية هو

m =12-7 = 5 = e

plain text = s e c u r i t y

cipher text = z l j b y p a f

.....

2- Reciprocal (Standard Reversal) Cipher:

لو فرضنا بشكل عام اي نص من الاحرف الهجائية =P

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

بشكل عام

نص مشفر مقابل :C

Z Y X W V U T S R Q P O N M L K J H G F E D C B A

على هذا الاساس يمكننا كتابة معادلة تشفير النص بالتعويض أو الشفرة العكسية كالأتي:

C=27 – m

OR

C=E (m)= (27 - m) mod 26

مثال:-

P : c o m p u t e r

C : X L N U F G V T

توضيح :الحرف الاول هو C اي بموقع الرقم 3 من الاحرف E حسب قانون التشفير العكسي للتعويض

C_1= 27 - m $\Longrightarrow$ 27 - C = 27 - 3 = 24 = X

C_2 =27 – m $\Longrightarrow$ 27 - O = 27 - 15 =12 =L

اذن C تحول الى Xو O تحولت الى L وهكذا

(27 -15) = 12= L

للحصول على النص الاصلي المعكوس (Reversal) نتبع ال قانون التالي:-

P = E (c)= (27-c) mod 26

OR

m = 27 - c

Example: Cipher the word (university) by use reversal substitution ?

P : U N I V E R S I T Y

C : F M R E V I H R G B

P_1=plain 1=U^{21}

بمعنى ان الحرف U يقع في الموقع رقم 21 من الحروف الابجدية نقوم بطرح 21من 26نحصل على 6

=6=F

P_2=n^{14}

C_2= 27 -14 =13=M

P_3 =i^{9}

C_3 =27- 9 = 18 = R

P_4=v^{22}

C_4 = 27 -22 = 5 = E

P_5 = E^9

C_5 = 27 - 5 = 22 =V