بسم الله الرحمن الرحيم

محاظره في بعض طرق التشفير

عباره عن تقرير لمحاظره الدكتوره ندى حسين في مادة الامنيه في جامعة بغداد في قسم علوم الحاسبات المرحله الثالثه

الطالب

محمد نجم عبد الرضا الدراجي

السنه الدراسيه

2013 - 2012

اهداء

الى مقام سيدي ومولاي الامام المهدي عجل الله تعالى فرجه وسهل مخرجه

والى امي والى ابي والى اخوتي والى زوجتي وابني وجميع اصدقائي

لاتنسونا بالدعاء لي ولوالدي وجميع المومنين

استقبل ارائكم على hitman9090@ymail.com

او على ٠٧٧٠٠٨٠٥٩٧٦

Simple substitution (keyword)

اي حرف متكرر اتخلص من التكراروانزل باقي الحروف

مثال// keyword = cryptographic system

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

K: c r y p t o g a h I s e m b d f j k l n q u v w x z

نزلنا حروف ال keyword بدون تكرار

لتشفير كلمة **cryptography** تعطي نص مشفر **ykxfndgkcfax** حيث كل حرف في ال p ياخذ الحرف المقابيله في ال k

اما اذا اردنا فك التشفير فناخذ كل حرف من النص المشفر مايقابله في ال p

Simple substitution (shift alphabets)

حيث ناخذ كل حرف ونجمعه مع المفتاح يعطي موقع لحرف جديد $f(a) = (p + k) \bmod 26$

مثال // لو كان المفتاح لدينا ٣

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

c: d e f g h I j k l m n o p q r s t u v w x y z a b c

وايضا تسمى هذه الشفره بشفرة قيصر(caeser)

اما اذا اردنا ان نفك الشفره ناخذ الحرف ونطرحه من المفتاح وناخذ ال mod 26

$f(a) = (p - k) \bmod 26$

Simple substitution (multiplication)

ناخذ كل حرف ونضربه بال key وناخذ ال mod 26 يطلع حرف جديد ولكن يجب ان يكون $\gcd(k,26)=1$ العامل المشترك الاكبر

$f(a) = (p * k) \bmod 26$

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

C: a j s b k t c l u d .....r

Simple substitution (affine transformation (shift + multiplication))

بسهوله حيث ناخذ الحرف نظربه في k1 ونجمعه مع k0 ومن ثم ناخذ ال mod 26 ولكن يجب ان يكون gcd(k1,26)=1 العامل المشترك الاكبر

$$f(a) = (p * k1 + k0) \bmod 26$$

homophonic substitution ciphers

ناخذ نص من كتاب يحتوي على ١٠٠ حرف او اكثر ومن ثم نستخرج مواقع الحروف وكل واحد نضع تحته التسلسلات وعند التشفير ناخذ احد هذه التسلسلات لتنوب عن الحرف

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
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02

مثال //

p: computer

C: 13 00 22 38 08 17 14 29

Polyalphabetic substitution cipher(vigenere cipher)

ناخذ المفتاح ونكرره بقدر الحروف ومن ثم ناخذ تسلسل حرف من المفتاح ومن الابجديه نجمعهم ومن ثم ناخذ ال mod 26 يطلع حرف جديد في الابجديه

مثال //

المفتاح deceptive

النص المراد تشفيره we are discovered save yourself

Key:deceptivedeceptivedeceptive

P: wearediscoveredsaveyourself

C:zicvtwqngrzgvtwavzhcqyglmgj

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
p	22	4	0	17	4	3	8	18	2	14	21	4	17	4
c	25	8	2	21	19	22	16	13	6	17	25	6	21	19

تكملة الجدول

key	19	8	21	4	3	4	2	4	15	19	8	21	4
p	3	18	0	21	4	24	14	20	17	18	4	11	5
c	22	0	21	25	7	2	16	24	6	11	12	6	9

حيث حرف ال d تسلسله هو الثالث ناخذه من ال key ناخذ حرف ال w من ال pحيث تسلسله هو ال 22 فتكون المعادله z= 25 =26 mod (22 + 3) وهكذا ونكمل لبقية الحروف

Polygraphic substitution cipher (playfair cipher)

نكون مصفوفه مربعه مثل 5*5 ونمليها من حروف المفتاح بدون تكرار ونكمل بقية الحروف في الابجديه

مثال //

m	o	n	a	r
c	h	y	b	d
e	f	g	i / j	k
l	p	q	s	t
u	v	w	x	z

بعد ذلك ناخذ حروف النص ونقسمها على مجاميع حيث كل مجموعه تتكون من حرفين وكل حرفين مكررين نضع بيناتهم X واذا بقى حرف واحد بالاخير ايضا نضع x بعد ذلك ناخذ الحرفين ونحدد اين موجودين اذا على نفس الصف حيث كل حرف ياخذ اللي على يمينه

اما اذا كان الحرفين على نفس العمود حيث كل حرف ياخذ الحرف اللي جواه

اما اذا كان الحرفين يقعان على اطراف القطر الرئيسي حيث كل حرف ياخذ نظيره بالقطر الثانوي في المثال التالي استخدمنا المصفوفه العليا

مثال //

P : meet me at home to night

D : me xe tm ea th om et on ig ht

C: cl ui lr im pd no kl na ki dp

اما اذا اردنا فك الشفره حيث نتبع نفس المصفوفه والطريقه المستخدمه بالتشفير وايضا نرى الحرفين هم على نفس الصف ناخذ الموجود على يسار الحرف اما اذا الحرفين على نفس العمود كل حرف ياخذ الذي فوقه اما اذا الحرفين على القطر الرئيسي كل واحد ياخذ المقابيله على القطر الثانوي

Polygraphic substitution cipher (hill cipher)

يكون المفتاح عباره عن مصفوفه مربعه (n*n) حيث كلما زاد حجم المصفوفه المفتاح يكون افضل لانه سوف يصعب عملية فك الشفره من قبل المهددين

طريقه التشفير هي ناخذ نص معين ومن ثم نقسمه الى مجاميع حيث نفرض لو كانت مصفوفة المفتاح هي طريقه التشفير هي ناخذ نص معين ومن ثم نقسمه الى مجاميع حيث نفرض لو كانت مصفوفة المفتاح هي 3*3 فان كل مجموعه سوف تضم ثلاثة حروف وبعد ذلك ناخذ ترتيب الحروف في الابجديه ومن ثم نظرب المصفوفه التي تمثل مجموعة الحروف في مصفوفه المفتاح ومن ثم ناخذ ال mod 26 لنحصل على ارقام جديده تمثل ارقام لحروف في الابجديه

مثال//

لو كان لدينا النص paymonemoney واردنا تشفيره وكانت عندنا المصفوفه 3*3 هي مصفوفه المفتاح

$$K=\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

حيث نقسم النص الى ثلاثه حروف pay mon emo ney

وناخذ اول مجموعه وهي pay وتكون مصفوفتها هي (15 0 24)

ونجري عملية الظرب بين المصفوفتين وتذكر كل صف من مصفوفه الحروف يظرب بعمود من مصفوفه المفتاح

$$(15\ \ 0\ \ 24) * \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} = (303\ \ 303\ \ 531)\ \mathrm{mod}26$$

حيث نكرر العمليه لكل مجموعه وناتج المجموعه الاولى هو (11 17 17) وهي الحروف (rrl)

الناتج النهائي للكل المجاميع هو rrl mwb kas pdh

ولترجيع النص المشفر الى النص الاصلي نفس الطريقه لكن نستخدم inverse لمصفوفة المفتاح في عملية الظرب

Transposition (simple or columnar transposition)

يعطى مفتاح على اساس هذا المفتاح نقسم النص المراد تشفيره

حيث ننزل النص المراد تشفيره على شكل سطر سطر ومن ثم نرتب على اساس المفتاح

مثال // المفتاح 3 1 4 2

النص المراد تشفيره cryptography

3	1	4	2
C	r	y	p
T	o	g	r
A	p	h	y

حيث نرتب حروف المفتاح ومن ثم ننزل العمود الذي تحته من الاحرف

يصبح الناتج

Rop pry cta ygh

1 2 3 4

وفي بعض الاحيان يعطى المفتاح على شكل حروف فيحول الى ارقام عن طريق تسلسل الحروف مثل اعطى المفتاح code فيحول الى 3 2 4 1 لان حرف ال c هو قبل الحروف الاخرى فاعطى واحد وحرف ال o هو اخر حرف فاعطى 4 والباقي نفس الطريقه

في عملية فك الشفرة فقط ننزل عمود عمود ونرتب على اساس المفتاح ومن ثم ناخذ عمود عمود

ملاحظه // اذا وزعنا الحروف على الاعمده والصفوف وبقي صف لم تكتمل اعمدتة يمكن اضافة حرف x الى المكانات الخاليه

A fixed period d with a permutation function

يعطى مفتاح على اساس هذا المفتاح نقسم النص المراد تشفيره

حيث ننزل النص المراد تشفيره على شكل سطر سطر ومن ثم نرتب على اساس المفتاح كل سطر على حدى

مثال // المفتاح 2 4 1 3

النص المراد تشفيره cryptography

2	4	1	3
C	r	y	p
T	o	g	r
A	p	h	y

حيث ناخذ كل سطرونرتبه على اساس المفتاح مثل السطر الاول نبدء بالترتيب حيث ماموجود بالعمود الثاني نضعه في الاول ومن ثم ماموجود بالرابع نضعه بالثاني ومن ثم ماموجود بالاول نضعه في الثالث وماموجود بالثالث نضعه بالرابع وهكذا لبقية السطور ولاحظ الترتيب حسب المفتاح

الناتج النهائي

Rpcy ortg pyah

ملاحظه // اذا وزعنا الحروف على الاعمده والصفوف وبقي صف لم تكتمل اعمدتة يمكن اضافة حرف x الى المكانات الخاليه

Rail fence

في هذه الطريقه يتفق الطرفين على عدد الصفوف (rails)

طريقة التشفير سهله حيث ننزل النص المراد تشفيره عمود عمود ونقراء سطر سطر

مثال // rail 3 هو عدد الصفوف

النص المراد تشفيره this is a secret message

T s a c t s g

H I s r m s e

I s e e e a x

ناتج التشفير tsactsg hisrmse iseeeax

ولعملية فك الشفره

ننزل سطر سطر ونقراء عمود عمود

ملاحظه // اذا وزعنا الحروف على الاعمده والصفوف وبقي صف لم تكتمل اعمدتة يمكن اضافة حرف x الى المكانات الخاليه

R S A

نختار رقمين كبيرين p , q على شرط ان يكون الرقمين prime

نجد ال n حيث ال $n = p * q$

نجد ال $Q(n) = (p-1) * (q-1)$ وهي دالة اويلر توشن

نجد ال e وهو المفتاح العام الذي نستخدمه في عملية التشفير نفرض رقم حيث

ال $1 < e < Q(n)$ ويجب ان يكون $\gcd(e , Q(n)) = 1$

نجد ال d وهو المفتاح الخاص الذي نستخدمه في عملية فك الشفره نفرض رقم

حيث ال $(d * e) \bmod Q(n) = 1$

مثال // p = 3 , q =11

N = p * q =3 * 11 = 33

Q(n) = (p-1) * (q-1) = (3 -1) * (11-1) =20

نفرض ال e = 7

نفرض ال d = 3

في عملية التشفيرنتعامل مع e and n لناخذ حرف ال c صاحب التسلسل 02 ونشفره

$02^{e} \bmod n = 02^{7} \bmod 33 = 29$

وهو الرقم الجديد

اما في عملية فك الشفره نتعامل مع d and n لناخذ ال 29 ونفك الشفره له

$29^{d} \bmod n = 29^{3} \bmod 33 = 2$ وهو الرقم الاصلي قبل التشفير