المملكة العربية السعودية
وزارة التعليم العالي
جامعة الملك سعود
كلية المعلمين
قسم الحاسب

Kingdom of Saudi Arabia
Ministry of Higher Education
King Saud University
Teacher's College
Computer Department

أمـن المعلومات

Information Security

المحاضرة الثالثة:.

الأحد 1429/11/11

إعداد الأستاذ:.

عبدالله بن شائع بيهان

التشفير Encryption

التشفير :يمكن تعرف التشفير بأنه عملية تحويل المعلومات إلى نص غير مفهوم لمنع الأشخاص غير المرخص لهم من الإطلاع على المعلومات أو فهمها.[1]

وهو يعني تغيير مظهر المعلومات المرسلة بحيث يختفي معناها الحقيقي.

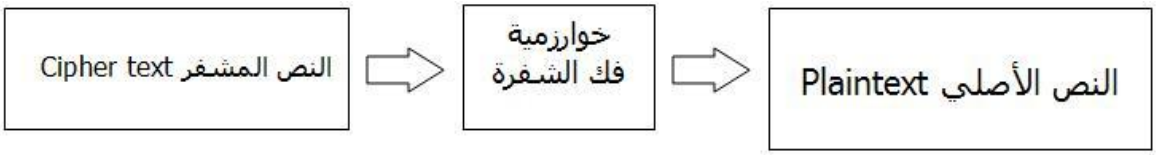
فلو كان لدينا رسالة لا نود لأحد الاطلاع إليها وأردنا إرسالها فسوف نلجأ في هذه الحالة إلى ما يسمى بالتعمية(وهو لفظ عربي) فإذا وقعت بيد طرف ثالث فلن يفهم منها شيئاً لأنها مشفرة بلغة غريبة عليه ولا يعرفها سوى الطرفين المرسل والمستقبل.

إن التشفير هو وسيلة الحفاظ على أمن المعلومات في وسط غير آمن وهو أهم حجر في بناء أمن المعلومات ولكنه ليس الحجر الوحيد على أية حال.[2]

إن أفضل وأنجع الوسائل لضمان أمن المعلومات هو تعميتها أو ما يعرف بتشفيرها.[3]

*يتضح في الرسم التالي مفهوم التشفير:

وعملية فك التشفير كالتالي:

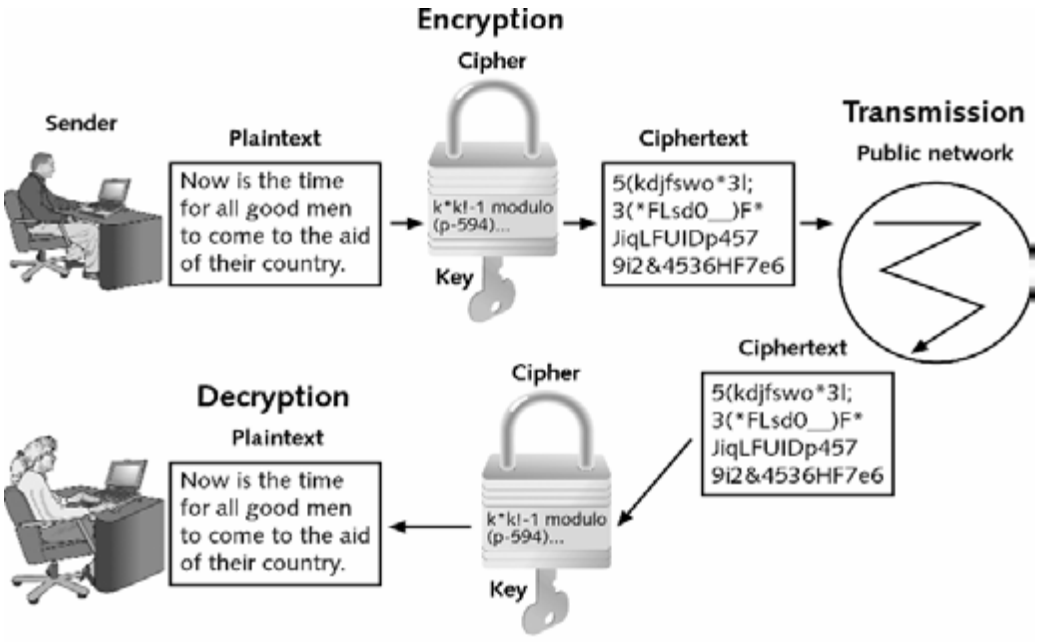


[1]

[2] الحاسب وأمن المعلومات – حسن طاهر داود

[3] المدخل إلى علم التشفير – د. محمد بن إبراهيم السويل

Steganography:إخفاء نص داخل ملف أخر (صورة، صوت، فيديو...)
Encryption: تغيير النص الأصلي المقروء إلى نص غير مقروء باستخدام أحد الخوارزميات.
Decryption: إعادة النص الغير مقروء إلى نص مقروء باستخدام أحد .
Cipher:هي الخوارزمية المستخدمة لتحويل النص المقروء إلى نص غير مقروء .
Plaintext: هو النص الأصلي المقروء.
Ciphertext: هو النص المشفر الغير مقروء.



التشفير يضمن :

1. Confidentiality السرية
2. Authentication الوثوقية
3. Integrity سلامة الملف
4. Nonrepudiation عدم الإنكار

أنواع الخوارزميات المستخدمة في التشفير:

هناك العديد من الخوارزميات المستخدمة في تحويل النص المقروء إلى نص غير مقروء وبالعكس ، منها على سبيل المثال لا الحصر:

1. **Substitution ciphers (Simple Monoalphbvtic):**
   - **1.1. Julius Caesar.**
   - **1.2. Rot(13).**
2. **Use Formula.**
3. **Transposition Cipher.**
4. **Vernam Cipher.**

نأخذ الآن كل خوارزمية بالتفصيل:

1.1Julius Caesar.

وهي من أبسط طرق التشفير وهذه الطريقة تعتبر من أقدم طرق التشفير, وفكرة هذه الطريقة هي تبديل كل حرف بثالث حرف بعده مثلا .A=D))وهكذا, وهذا الجدول يوضح جميع الحروف:

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
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

الشرح:

لنأخذ على سبيل المثال النص الأصلي Plaintext هو **"AHMED ALI"** ونريد تشفيره, نقوم بتبديل كل حرف بثالث حرف بعده:
كما هو واضح في الجدول السابق فإن ثالث حرف بعد ال A هو , D وثالث حرف بعد ال H هو , K وهكذا إلى أن ينتج لنا النص المشفر:Cipher text

"DKPHG DOL"

1.2Rot(13).

وهي طريقة بسيطة أيضاً والفكرة هنا أن كل حرف سوف يُعمل له دوران بمقدار 13 حرف (علماً بأن الأحرف الأبجدية الإنجليزية هي 26 حرفاً لذا فنصفها هو 13) .
فمثلاً حرف A عندما نطبق ROT(13) فإن الحرف الناتج هو N وهكذا.

1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M

14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

الشرح:

لنأخذ على سبيل المثال النص الأصلي Plaintext هو " **AHMED ALI** " ونريد تشفيره, نقوم بتطبيق :ROT(13)
كما هو واضح في الجدول السابق فإن ناتج تطبيق ROT(13) على الحرف A هو N و ناتج التطبيق على حرف H هو U, وهكذا إلى أن ينتج لنا النص المشفر:Cipher text

"NUZRQNYV"

2.Use Formula.

في هذه الطريقة نستخدم معادلة رياضية لنحصل على تشفير النص، فإذا كانت المعادلة المستخدمة هي : **(((X² +3) -2) mod 26)+1.**
علماً بان قيمة x متغيرة حسب موقع الحرف وليست ثابتة.

فنجد أن حرف A يحتل الرقم 1 في الترتيب وعند تطبيق المعادلة نجد النتيجة هي حرف c وهكذا .

الشرح:

لنأخذ على سبيل المثال النص الأصلي Plaintext هو " **AHMED ALI** " ونريد تشفيره, نقوم بتطبيق المعادلة لكل حرف كما هو واضح في الجدول التالي
فإن ناتج تطبيق المعادلة على الحرف A هو c و ناتج التطبيق على حرف H هو N, وهكذا إلى أن ينتج لنا النص المشفر:Cipher text

" CNOARCPE"

A	H	M	E
$(((1^2+3)-2) \bmod 26)+1$ =3	$(((8^2+3)-2) \bmod 26)+1$ =14	$(((13^2+3)-2) \bmod 26)+1$ = 15	$(((5^2+3)-2) \bmod 26)+1$ =1
C	N	O	A

D	A	L	I
$(((4^2+3)-2) \bmod 26)+1$ =18	$(((1^2+3)-2) \bmod 26)+1$ =3	$(((12^2+3)-2) \bmod 26)+1$ =16	$(((9^2+3)-2) \bmod 26)+1$ =5
R	C	P	E

3.Transposition Cipher.

في هذه الطريقة نستخدم مفتاح للتشفير ، حسب الجدول التالي:

المفتاح key
الترتيب الأبجدي للمفتاح
بداية توزيع النص المقروء

الشرح:

لنأخذ على سبيل المثال النص الأصلي Plaintext هو " **AHMED ALI** " نريد تشفيره ,والمفتاح وه و **TCR**
ثم نبدأ بتفريغ النص داخل الجدول حرف حرف وذلك بشكل أفقي، ثم نأخذ العمود الذي حمل الرقم 1 وهو HDİ ثم العمود الذي يحمل الرقم2 وهو MA
وهكذا إلى أن ينتج لنا النص المشفر:Cipher text,
"**HDİMAAEL**"

T	C	R
3	1	2
A	H	M
E	D	A
L	I	

4.Vernam Cipher.

في هذه الطريقة سوف نستخدم مفتاح للتشفير ولكن الذي يميز هذه الطريقة عن Transposition هو أن كل حرف سوف يكون له مفتاح خاص بحيث يتم جمع الرقم الذي يحمله الحرف الأول مع الرقم الذي يحمل الحرف الثاني ومن ثم MOD 26 ومن ثم نحصل على رقم وبالتالي نحصل على الحرف الذي يطابق هذا الرقم، مثلا A = 1 و حرف M=13

A + M mod 26 = 1 + 13 mod 26 = 14 mod 26 = 14 = N

وهكذا البقية.

الشرح:

على سبيل المثال النص الأصلي Plaintext هو " **AHMED ALI** " نريد تشفيره ,والمفتاح وه و **MOHAMMED**

نطبق الطريقة على الحرف الأول من النص وهو A مع الحرف الأول من المفتاح وهو M فينتج الحرف N و الثاني من النص وهو H مع الحرف الثاني من المفتاح وهو O فينتج w

وهكذا إلى أن ينتج لنا النص المشفر:Cipher text,

"**NWUFQNQM**"

A	**H**	**M**	**E**	**D**	**A**	**L**	**I**
M	**O**	**H**	**A**	**M**	**M**	**E**	**D**
A+M= 1+13=14	**H+O= 8+15=23**	**M+H= 13+8=21**	**E+A= 5+1=6**	**D+M= 4+13=17**	**A+M= 1+13=14**	**L+E= 12+5=17**	**I+D= 9+4=13**
N	**W**	**U**	**F**	**Q**	**N**	**Q**	**M**

End The

Third Lecturer

أمـن المعلومات

Information Security