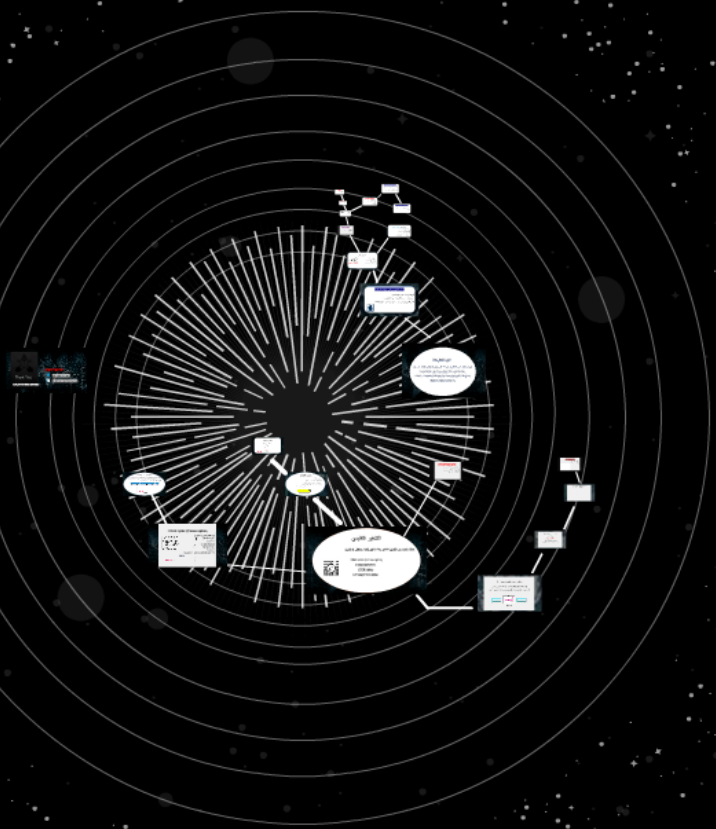
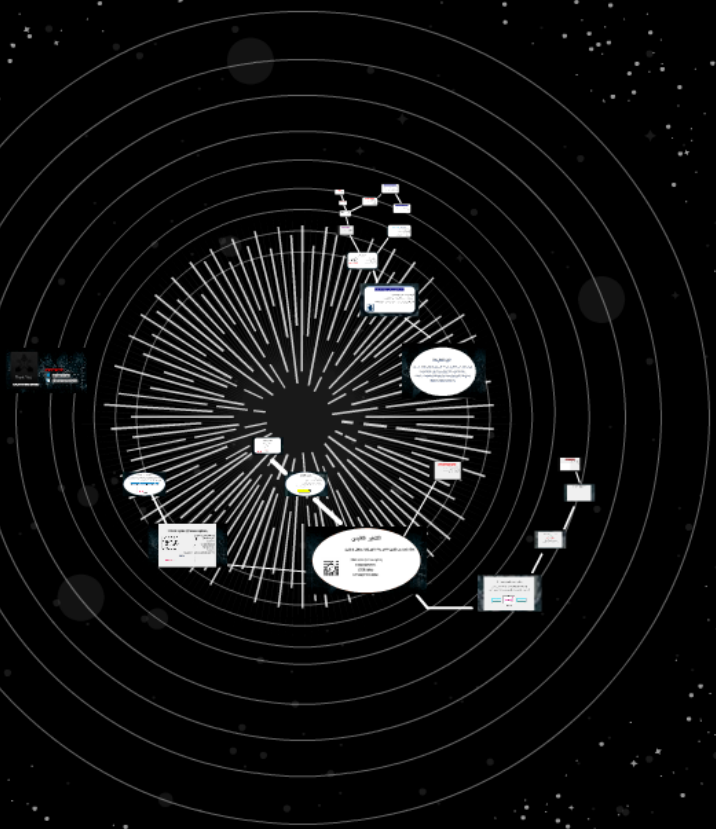


امن المعلومات

أ. رهف منصور الحسيان

- ما هو امن المعلومات.
- ما الفرق بين حمايات المعلومات.
- مفاهيم الموجود الأمني
- التشفير بأربع طرق
Shift cipher -
Monoalphabetic cipher -
XOR Cipher -
Transposition Cipher -



امن المعلومات

أ. رهف منصور الحسيان

- ما هو امن المعلومات.
- ما الفرق بين حمايات المعلومات.
- مفاهيم الموجود الأمني
- التشفير بأربع طرق
Shift cipher -
Monoalphabetic cipher -
XOR Cipher -
Transposition Cipher -

امن المعلومات

أ. رهف منصور الحسينان

- ما هو امن المعلومات
- ما الفرق بين حمايات الحاسوبات
- ماهو الهجوم الامني
- التشفير بأربع طرق

Shift cipher -

Monoalphabetic cipher -

XOR Cipher -

Transposition Cipher -

امن المعلومات

هي الحماية الممنوحة لنظام المعلومات الآلي من أجل تحقيق الأهداف المعمول بها للحفاظ على سلامة وتوافر وسرية موارد نظام المعلومات (بما في ذلك الأجهزة والبرمجيات والبرامج الثابتة والمعلومات / البيانات ، والاتصالات السلكية واللاسلكية).

ما هو الفرق بين أمن أجهزة الكمبيوتر؟

أمن المعلومات: حماية البيانات حاليا.

أمن الشبكات : حماية البيانات عبر شبكة الإنترنت.

الأمن السيبراني: مزيج من كل من امن المعلومات و امن الشبكات.

ما هو الهجوم الأمني

مبني للمجهول (Passive)

- محاولات لتعلم أو الاستفادة من المعلومات من النظام

ولكن لا يؤثر على موارد النظام.

- الهدف هو الحصول على المعلومات فقط بدون تغير البيانات.

هجوم نشط (Active)

- محاولات لإدخال بعض التعديلات على البيانات أو تغير في البيانات.

هذا النوع من الهجوم هو أسهل للكشف

أهداف الفيروسات Targets of viruses

تؤثر بعض الفيروسات على البرامج الفردية ؛

لذلك ، يمكن أن يكون هناك نسخة من الفيروس في كل برنامج على الكمبيوتر.

تؤثر الفيروسات الأخرى على نظام التشغيل ؛

لذلك ، يمكن أن يكون هناك نسخة من الفيروس على كل قرص كمبيوتر.

بعض الفيروسات تعتمد على النظام الأساسي:

يمكن أن تعمل فقط داخل نظام تشغيل واحد محدد

(من هذه الفيروسات ، 99٪ موجهة ضد النظام الأساسي للكمبيوتر الشخصي).

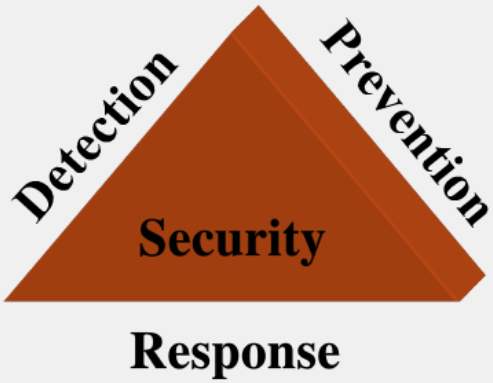
الفيروسات الأخرى مستقلة عن النظام الأساسي:

هذه هي فيروسات الماكرو ، تعمل ضمن بيئة عبر الأنظمة الأساسية مثل MS Word

مثلث الامن (Security Trinity)

يعتمد الأمن على:

- المنع (Prevention)-
- الكشف (Detection)-
- الاستجابة (Response)-



الفرق بين التهديد "Threat" و الهجوم الأمني " Security attack"

- **التهديد "Threat"**

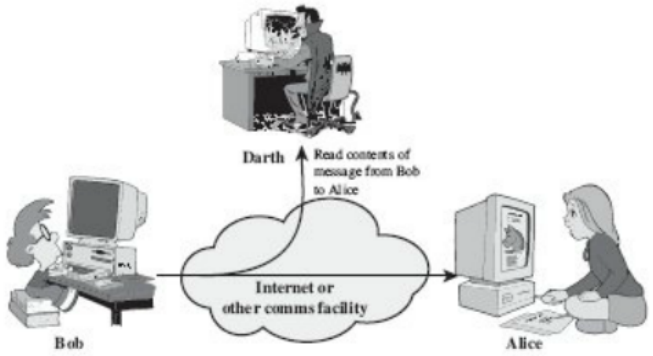
انتهاك الأمن ، والذي يوجد عندما يكون هناك ظرف

أو قدرة أو إجراء أو حدث يمكن أن ينتهك الأمن

ويسبب الضرر.

أي أن التهديد خطر محتمل قد يستغل الثغرة الأمنية.

❖ الهجوم الأمني " Security attack"
هو أي إجراء يتضمن أمان المعلومات المملوكة لمنظمة



Security Services خدمات الأمن

1. السرية / الخصوصية Confidentiality/Privacy :

يضمن عدم إتاحة المعلومات الخاصة أو السرية أو الكشف عنها للأفراد غير المصرح لهم.

2. النزاهة Integrity :

يؤكد أن المعلومات والبرامج لا تتغير إلا بطريقة محددة ومعتمدة.

3. المصادقيه Authentication :

يحتاج المتلقي إلى التأكد من هوية المرسل.

4. عدم الإهمال Nonrepudation :

يجب ألا يتمكن المرسل من رفض إرسال رسالة أرسلها في الواقع.

5. التوافر Availability :

يضمن أن الأنظمة تعمل على الفور ولا يتم رفض الخدمة للمستخدمين المصرح لهم.

خدمات امن المعلومات ، امن الشبكات ، امن السيبراني

سرية الرسالة Message confidentiality :

جب أن تكون الرسالة المرسلة منطقية للمستقبلين المقصودين فقط. عندما تتواصل الزبون مع مصرفها ، تتوقع أن تكون الاتصالات سرية تمامًا.

تكامل الرسالة Message Integrity :

يجب أن تصل البيانات إلى جهاز الاستقبال تمامًا كما تم إرسالها. على سبيل المثال ، سيكون من الكارثي إذا تغير طلب تحويل 100 دولار إلى طلب بمبلغ 10000 أو 100000 دولار. يجب الحفاظ على سلامة الرسالة في اتصال آمن.

مصادقية الرسائل Message authentication :

تأكد من هوية المستخدم وأن المحتال لم يرسل الرسالة.

خدمات امن المعلومات ، امن الشبكات ، امن السيبراني

عدم رفض الرسالة Message nonrepudiation :

يعني أنه يجب ألا يتمكن المرسل من رفض إرسال رسالة أرسلها بالفعل.
فمثلا،

عندما يرسل العميل رسالة لتحويل الأموال من حساب إلى آخر ، يجب أن يكون لدى البنك دليل على أن العميل قد طلب هذه المعاملة بالفعل.

ما هو التشفير "Cryptography" ؟

كلمة ذات أصول يونانية ، تعني "الكتابة السرية".

تشير إلى علم نقل الرسائل لجعلها آمنة ومحصنة ضد الهجمات.

اهم الكلمات للتشفير

نص عادي "Plaintext": الرسالة الأصلية قبل أن يتم تحويلها.

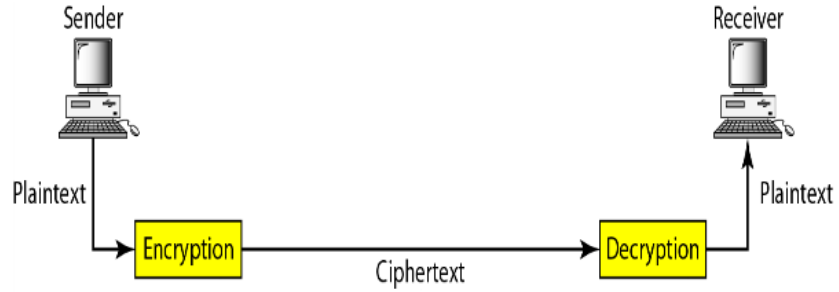
النص المشفر "Ciphertext" : الرسالة بعد التحويل (مشفرة).

التشفير "Cipher" : خوارزمية لتحويل النص العادي إلى نص مشفر

المفتاح"Key" : المعلومات المستخدمة في التشفير معروفة فقط للمرسل / المتلقي

تشفير"Encrypt ": تحويل نص عادي إلى نص مشفر

فك تشفير"Decrypt ": استعادة نص عادي من نص مشفر



التشفير التقليدي

هناك العديد من الطرق لتشفير وفك تشفير لكننا سنناقش 4 طرق:

1.Shift cipher (Caesar cipher).

2.Monoalphabetic .

3.XOR cipher .

4.Transposition cipher .

1.Shift cipher (Caesar cipher)

في هذا التشفير ، خوارزمية التشفير هي:

"تبديل الأحرف لأسفل"

المفتاح هو N

خوارزمية فك التشفير هي :

"تبديل الأحرف لأعلى"

المفتاح هو N

مثال: استخدم مفتاح التشفير مع المفتاح = 15 لتشفير رسالة:

Hello

ANSWER:- WTAAD

2.Monoalphabetic

حيث يتم دائمًا تغيير حرف (أو رمز) في النص العادي إلى نفس الحرف (أو الرمز) في النص المشفر بغض النظر عن موضعه في النص.

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

Examples#1 :

Plaintext: HELLO

ANSWER:

Ciphertext: KHOOR

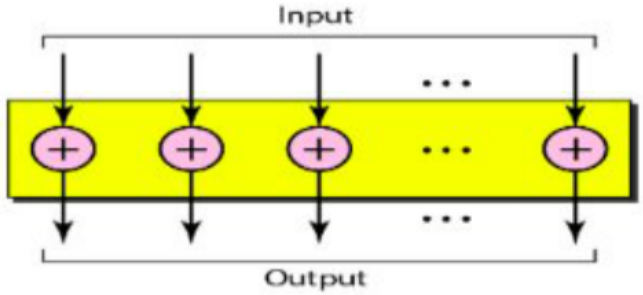
3.XOR cipher

تحتاج عملية XOR

إلى إدخالين للبيانات: نص عادي ومفتاح.

حجم النص العادي والمفتاح ونص التشفير هو نفسه.

لها خاصية مثيرة للاهتمام للغاية: التشفير وفك التشفير هي نفسها.



3.1.XOR cipher

Example:

Block: 01101010

XOR

Key: 10101100

ANSWER:

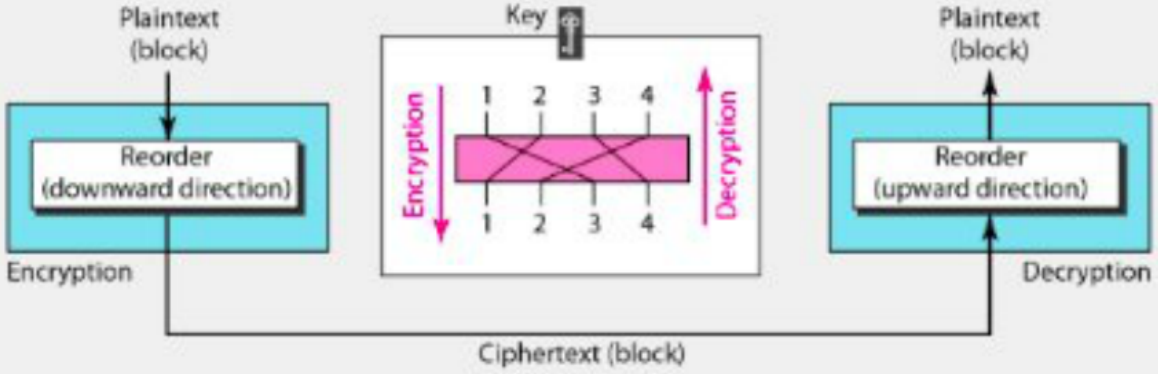
11000110

إذا كانت الأرقام مختلفة = 1
إذا كانت الأرقام متساوية = 0

4.Transposition cipher

يقوم بإعادة ترتيب (يتخلل) الرموز في مجموعة من الرموز.

المفتاح هو مناظرة بين موضع الرموز في النص العادي ونص التشفير.



4.1.Transposition cipher

Example :

تشفير هذه الرسالة :

"HELLO MY DEAR"

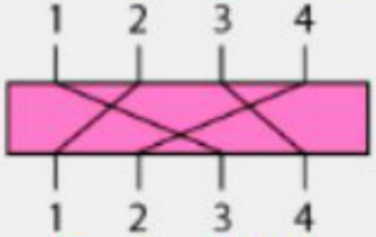
باستخدام المفتاح الموضح في الشكل السابق.

النتيجة بعد تقسيم الكلمة وفقًا لحجم المربع وهي 4: 4

4.1.Transposition cipher

= HELL OMYD EARZ.

E A R Z
O M Y D
H E L L



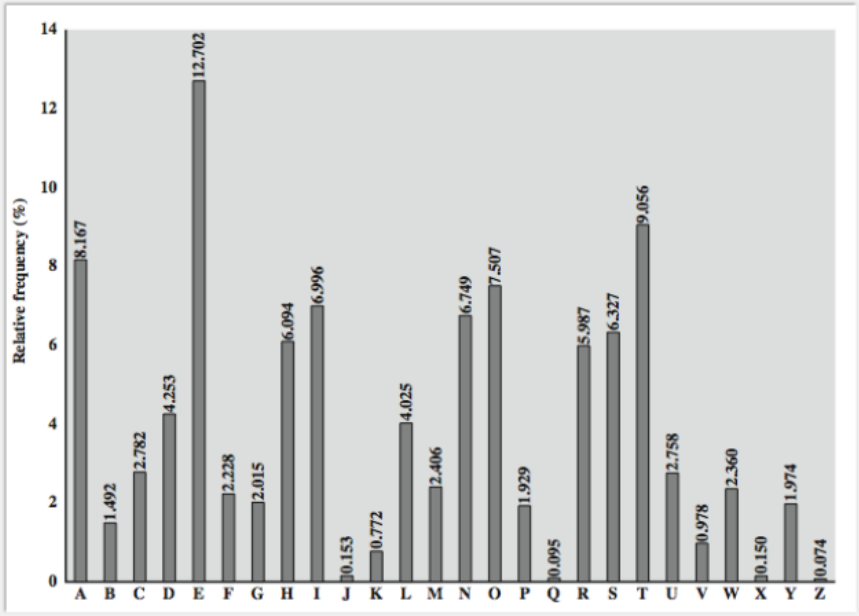
E L H L
M D O Y
A Z E R

ANSWER: ELHLMDOYAZER

سبب اختيار حرف Z او X ؟

الرسم البياني يوضح اقل الاحرف تكرار هي :

- Z
- X
- Q
- J



ما سبب أهمية أمن المعلومات والشبكات؟

- حماية أصول الشركة (الأجهزة والبرمجيات).
- اكتساب ميزة تنافسية: تطوير الإجراءات الأمنية الفعالة والحفاظ عليها

يمكن أن يمنح المنظمة ميزة تنافسية على منافستها.

- الحفاظ على وظيفتك: لتأمين منصب واحد داخل المنظمة ولضمان مستقبل مهني ،

من المهم وضع تدابير تحمي الاختبارات التنظيمية.

Thank You!

L. Rahaf Mansour AlHusainan

For personal contact:

@RahafAlHusainan

Rahaf Mansour AlHusainan

Thank You!

L. Rahaf Mansour AlHusainan

For personal contact:

@RahafAlHusainan

Rahaf Mansour AlHusainan

امن المعلومات

أ. رهف منصور الحسيان

- ما هو امن المعلومات.
- ما الفرق بين حمايات المعلومات.
- مفاهيم الموجود الأمني
- التشفير بأربع طرق
Shift cipher -
Monoalphabetic cipher -
XOR Cipher -
Transposition Cipher -