****

**تقرير حلقة بحث (أو مشروع) بعنوان :**

**علم التشفير** **( أهدافه، مبادئه، أساليبه )**

Cryptography

**(** It's Goals, Principals and Methods **)**

تقديم الطالب : مارك مروان جبور

الصف : الأول ثانوي

مقرر : المعلوماتية

تاريخ : 15 / 1 / 2015

إشراف الآنسة : ميس

**ملخص**

يهتم البحث أساسا بقضية التشفير لما لها من دور حيوي وأساسي في جميع مجالات الحياة النظرية والتطبيقية، وذلك منذ القدم وحتى وقتنا الحاضر. وفي هذا السياق يحاول البحث الإجابة على التساؤلات التالية :

* ما هي المجالات الرئيسية للتشفير .. كيف بدأ وكيف أصبح في الوقت الحاضر ؟
* ما هي أهم استخداماته قديماً ؟ وكذلك أهم تطبيقاته المعاصرة ؟
* ما هي الشروط التي تجعل من نظام التشفير قوياً وملائماً ؟
* ما هي أسس كسر أنظمة التشفير ؟ وهل هناك من أنظمة لا تقبل الكسر ؟؟

|  |  |  |
| --- | --- | --- |
| **الفقرة** | **قائمة الموضوعات** | **رقم**  **الصفحة** |
|  | مقدمة عامة للبحث .......................................... | 2 |
|  |  |  |
|  | **الباب الأول : التشفير ومفاهيمه الرئيسية** | 3 |
|  |  |  |
|  | مقدمة ......................................................... | 3 |
| 1.1 | الفصل الأول : مجالي التشفير أهدافه الرئيسية .................. | 3 |
|  | الأهداف الرئيسية لاستخدام علم التشفير ......................... | 4 |
| 1. 2 | الأساليب العامة للتسفير ......................................... | 4 |
|  | التشفير الكلاسيكي ***Classical Encryption*** ...................... | 4 |
|  | التشفير بالمفتاح المتناظر ***Symmetric Encryption*** ............. | 5 |
|  | التشفير غير المتناظر ***Asymmetric Encryption*** ................. | 6 |
|  |  |  |
|  | **الباب الثاني : التشفير الكلاسيكي** | 7 |
|  |  |  |
|  | مقدمة ........................................................... | 7 |
| 1.2 | الفصل الأول : التشفير بالإزاحة ***Shift Cipher*** ................... | 7 |
|  | مهاجمة القوة العمياء ............................. | 8 |
| 2.2 | الفصل الثاني : ***Affine Cipher*** ................................. | 9 |
| 2. 3 | تعمية للاستبدال ***Substitution Cipher*** ............. | 9 |
| 2. 4 | الفصل الرابع : ***Letter Frequency Analysis*** .................... | 10 |
| 2. 5 | الفصل الخامس : المبادئ الأساسية لعلم تحليل الشفرات  ***General Thought In Cryptanalysis ................*** | 11 |
|  | أنواع الهجمات ................................................... | 12 |
|  | الهجوم غير النشط ***Passive Attack*** .............................. | 12 |
|  | الهجوم النشط ***Active Attack*** .................................... | 12 |
|  | الشفرات الآمنة ***The One – Timed Pad*** ......................... | 13 |
|  |  |  |
|  | **الباب الثالث : موجز عن التشفير غير الكلاسيكي** | 18 |
|  |  |  |
|  | مقدمة ........................................................... | 18 |
| 3. 1 | الفصل الأول : التشفير بالمفتاح العام ***Public Key Cryptography ..*** | 14 |
| 3. 2 | الفصل الثاني : دالة التجزئة ***Hash Function*** ..................... | 15 |
| 3.3 | الفصل الثالث : التوقيع الإلكتروني ***Digital Signature*** ............ | 17 |
|  |  |  |
|  | **الباب الرابع : النتائج العامة للبحث** | 18 |

**مقدمة عامة للبحث :**

بعد اختراع الكتابة تشكل عند الإنسان هدفا لما يكتب و مع تطور هذه الأهداف و اتسام بعضها بالخصوصية بدأ الإنسان بالتفكير بطريقة للحفاظ على خصوصية تلك الأهداف بحيث لا يفهمها إلا أشخاصا محددين وهكذا بدأ علم التشفير ومع محاولة البعض التطفل لمعرفة خصوصيات الآخرين أخذ من يحاول إخفاء تلك الخصوصيات بتطوير طريقة إخفائه ليتطور عبر ذلك علم التشفير.

تزايدت أهمية علم التشفير مع تطور الفكر البشري والتكنولوجي لإخفاء النصوص التي تحمل تلك الأفكار وتزايدت أهميته أكثر فأكثر مع تشكل الممالك والجيوش الضخمة ليلعب التشفير دورا حيويا في الحروب منذ القدم و مع تطور علم الرياضيات واختراع الحاسب الآلي تشكل التشفير الحديث الذي يختلف كثيرا عن سابقه وازداد الاهتمام به مع تطور الشبكات وظهور الشابكة وقد وجدت الطرق الحديثة لعدم ملائمة الطرق التقليدية للحاسوب الذي يتعامل مع الأصفار والواحدات لا مع أحرف الأبجدية ، لتتشكل بعض المفاهيم الحديثة كدالة التجزئة و التشفير العام والتوقيع الإلكتروني ...

**وهنا نطرح مجموعة من التساؤلات وفق ما يلي:**

* **ما هي المجالات الرئيسية للتشفير ؟؟**
* **كيف بدأ التشفير و كيف أصبح في العصر الحديث؟؟**
* **ماهي استخداماته قديما و ما هي تطبيقاته المعاصرة؟؟**
* **ما هي الشروط التي تجعل من نظام التشفير قويا و ملائما؟؟**
* **ما هي أسس كسر أنظمة التشفير؟؟**
* **و هل هناك نظام تشفير لا يقبل الكسر؟؟**

**تمثل الأسئلة السابقة الإطار العام للمشكلة البحثية وسنحاول الإجابة عليها تحقيقا لهدف البحث.**

**الباب الأول : التشفير و مفاهيمه الرئيسية**

**مقدمة:**

عرف علم التشفير أو ( التعمية ) **( *Cryptology* )** منذ القدم حيث استخدم في المجال الحربي والعسكري، وقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة منذ عام 2000 قبل الميلاد، وكان القصد هو إخفاء الشكل الحقيقي للرسائل حتى لو سقطت في يد العدو، وربما كانت طريقة القيصر جوليوس-التي سنأتي على ذكرها لاحقاً- من أفضل الطرق التي استخدمت في القدم. أما في عصرنا الحالي فقد باتت الحاجة ملحة لاستخدام هذه العلم " التشفير " وذلك لارتباط العالم مع بعضه عبر شبكات مفتوحة، حيث يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين أو بين المنظمات الخاصة والعامة عسكرية كانت أم مدنية، وعليه لا بد من طريقة تحفظ سرية هذه المعلومات ولا يزال العمل والبحث في مجال علم التشفير مستمراً وذلك بسبب التطور السريع للكومبيوتر والنمو الكبير للشبكات وبخاصة الشبكة العالمية الإنترنت.

**1. 1 الفصل الأول : مجالي التشفير وأهدافه الرئيسية**

**التشفير** هو العلم الذي يستخدم الرياضيات للتشفير وفك البيانات المشفرة وهو يدرج ضمن علوم الحوسبة والرياضيات، يمكنك التشفير من تخزين المعلومات الحساسة أو نقلها عبر الشبكات غير الآمنة – مثل الإنترنت – بحيث لا يمكن قراءتها من قبل أي شخص ما عدا الشخص المرسلة إليه. وعليه يمكن الإشارة إلى مجالين أساسيين لعلم التشفير**( *Cryptology* )** وفق الشكل التالي : **شكل (1)**

**Cryptology**

Cryptography

**Protocols**

**Symmetric**

**Ciphers**

Cryptanalysis

**Asymmetric**

**Ciphers**

**شكل (1) : مجالات علم التشفير**

* علم تحليل الشفرات **(*Cryptanalysis*)** : ويهتم هذا المجال بتحليل وفك التشفير بهدف كسر وخرق الاتصالات الآمنة، بمعنى هو العلم الذي يهتم بكسر خوارزميات التشفير وإيجاد نقاط الضعف وهو الطريقة الواحدة للتأكد من أمان خوارزمية التشفير.
* علم التشفير **(*Cryptography*)** : هو علم وممارسة إخفاء البيانات أي بخوارزميات تحويل البيانات (مثل الكتابة) من شكلها الطبيعي المفهوم لأي شخص إلى شكل غير مفهوم بحيث يتعذّر على من لا يملك مجموعة من البيانات معرفة معناه.

**الأهداف الرئيسية لاستخدام علم التشفير**

توجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي :

**السرية أو الخصوصية (: (*Confidentiality*** هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ماعدا الذي قد صرح لهما لإطلاع عليها.

**تكامل البيانات *Integrity*))** : و هي خدمة تستخدم لحفظ المعلومات من التغير(حذف أو إضافة أو تعديل)، وذلك من قبل الأشخاص غير المصرح لهم للقيام بالتغيير.

**إثبات الهوية (*Authentication*)** : هي خدمة تستخدم لإثبات هوية المتعامل مع البيانات (المصرح له).

**عدم الجحود *Non-repudiation* ))** : وهي خدمة تستخدم لمنع الشخص من إنكاره القيام بعمل ما.

وبناءً عليه ... إن الأهداف الرئيسية للتشفير هو أن يوفر للأشخاص تلك الخدمات المشار إليها أعلاه ليتم الحفاظ على أمن معلوماتهم.

**2.1 الأساليب العامة للتشفير**

**التشفير الكلاسيكي:** هو التشفير قبل اختراع الحاسب الآلي وكان بمثابة ولادة لعلم التشفير.وهنا اعتمدت الخوارزميات بشكل أساسي على إحلال أو إبدال حرف مكان آخر ( والجيدة منها كانت تقوم بالاثنين معاً )، لكن جميع هذه الخوارزميات كانت تعمل على الحروف فقط **(*Character - Based* )** أي على مدى 26 حرف وذلك بعكس الطرق الحديثة التي تعتمد على التعامل مع الـ **(*Bit* )**(0 أو1).[[1]](#footnote-1)

**التشفير بالمفتاح المتناظر(*Symmetric Cryptography*)** : وقد ظهر هذا الأسلوب مع الكلاسيكية لكنه استمر إلى مابعد اختراع الحاسب الآلي,أي أن الأنواع الأولى منها تعد كلاسيكية لكن توجد أنواع حديثة ضمنه غير كلاسيكية.

من خلال خوارزميات التشفير بالمفتاح المتناظر**((*Symmetric Algorithms***يتفاهم الطرفين على طريقة للتشفير وأخرى لفكه تتشاركان بمفتاح سري مشترك **(*Shared Secret*).**وهكذا نكون قد حولنا المشكلة من حفظ معلومات سرية إلى حفظ مفتاح سري.لها عدة أسماء نذكر منها **(*secret-key, single-key algorithms*).**لعل أفضل طريقة لشرحها وفهم آلية عملها من خلال هذا المثال :[[2]](#footnote-2)

شخصان (أليس) و (بوب)يريدان الحديث عبر قناة غير آمنة**(*insecure channel* )**المقصود هنا بـ : قناة هو وسيلة اتصال كالإنترنت,شبكة منزلية، ....)لكن شخص ثالث يدعى (أوسكار) يستطيع الوصول لهذه القناة مثلا باختراق الشبكة المنزلية،إذاً هو قادر على التصنت.

لكن أذا أراد (بوب و أليس) أن لا يتمكن (أوسكار) من فهم المعلومات فإن التشفير بالمفتاح المتناظر يؤمن الحل المناسب، حيث تشفر (أليس) الرسال (x) باستخدام خوارزمية للتشفير بالمفتاح المتناظر فينتج النص المشفر**((*cipher text***يتلقى (بوب)النص المشفر ويفك التشفير بحيث يكون فك التشفير عملية عكسية بالنسبة للتشفير.

وهكذا إذا كانت خوارزمية التشفير قوية فستبدو الرسالة لا معنى لها (لأوسكار) لكن يجب أن يكون هناك قناة آمنة بين بوب و أليس ليتم الاتفاق على المفتاح. يمكن تمثيل ما جاء ذكره وفق الشكل التالي : **شكل (2)**

y

k

k

y

**Oscar**

**( bad )**

**Alice**

**( good )**

**Bob**

**( good )**

x

**descryption**

**d()**

**Encryption**

**e()**

y

x

**Insecure Channel**

( ***e.g. Internet*** )

**Secure Channel**

**شكل (2) : رسم توضيحي لآلية التشفير بالمفتاح المتناظر**

**التشفير غير المتناظر(*Asymmetric Cryptography* )**

**أولاً** : في أواخر السبعينات تم في هذه المرحلة تطوير نظام التشفير في بريطانيا، وكان استخدامه حكراً على قطاعات معينة من الحكومة.

**ثانياً** :يعتمد في مبدأه على وجود مفتاحين للقيام بالتشفير وهما المفتاح العام **(*Public Key* )** والمفتاح[[3]](#footnote-3) الخاص **(*Private Key*)**، حيث أن المفتاح العام يرسل لجميع الناس، أما المفتاح الخاص الرسائل يحتفظ به صاحبه ولا يرسله لأحد. يعرف أحيانا بالمفتاح العام **(*public key*)** وقد سمي بالعام لأن أحد المفاتيح يبقى خاصا (يملكه فقط المشفر)والآخر ينشر للعامة.

كما تجدر الإشارة أيضاً إلى تعريف مصطلح هام جداً في علم التشفير وهو الـ : **( *Protocol* )** ... الذي يمكن توضيحه على الشكل :

تستخدم خوارزميات التشفير التناظري وغير التناظري كوحدات بناء لما يسمى الـ **( *Protocol* )** و الذي غالبا ما يضم الاثنين معا ( التناظري وغير التناظري ) لأن لكل منهما نقاط ضعف و نقاط قوة. ( يعتبر بروتوكول TLS(Transport Layer Security) المستخدم في جميع متصفحات النت مثالا عن البروتوكول ).

**ثالثاً** : من بعض الأمثلة على طرق التشفير بالمفتاح العام نذكر على سبيل الذكر فقط :

***PGP, DSA,Deffie-Hellman, Elgamal, RSA***

جميع الأنظمة السابقة تعتمد على مبدأ التشفير اللاتماثلي**(*Asymmetric Cryptography* )** أو التشفير باستخدام المفتاح العام والمفتاح الخاص.

**الباب الثاني :التشفير الكلاسيكي**

سيتناول البحث دراسة تفصلية تحليلية لمرحلتين أساسيتين في علم التشفير وذلك من خلال : ( ظهور المرحلة زمنياً – آلية وخصائص كل منها – أشهر الشفرات المتبعة فيها – أسلوب كسر هذه الشفرات ).

# 2. 1 الفصل الأول : التشفير بالإزاحة (*Shift Cipher*)

# تعد من أبسط وأشهر طرق التشفير التاريخية وقد شاع استخدام هذه الشيفرة قديماً، تعود ل 58 ق م .تقوم على إزاحة كل حرف من النص الأصلي بعدد ثابت من مواقع الأحرف بالأبجدية.فمثلا مثلا أذا أزحنا بثلاث مواقع A ستصبح Cلكن المشكلة الوحيدة هي في نهاية الأبجدية !! ماذا سنفعل ب X Y Z ؟ [[4]](#footnote-4)

# ستعود للبداية.. مما يعني X ستصبح A، وY ستبصحB ، و Z ستصبح C.يمكن تعريف هذه الشفرة بالشكل الآتي : شكل (3)

**Definition Shift Cipher**

***Let X, Y, K*€Z26.**

**Encryption :ek (x) = x +k mod 26.**

**Decryption :dk (y) =y +k mod 26.**

# حيث يرمز للأحرف بأرقام كما بالشكل :

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M13 | L12 | K11 | J10 | I9 | H8 | G7 | F6 | E5 | D4 | C3 | B1 | A0 |
| Z26 | Y25 | X24 | W23 | V22 | U21 | T20 | S19 | R18 | Q17 **شكل (3) : تعريف شفرة التشفير بالإزاحة** | P16 | O15 | N14 |

نلاحظ أن المفتاح (قيمة الإزاحة) يوجد بين (0 و 25) لأنه أذا كان أكثر من ذلك فلن يكون له معنى مثلا 27 إزاحة تساوي إزاحة واحدة حسب الشكل السابق أذا عدد احتمالات المفتاح 26 احتمال.مثال:

باستخدام المفتاح 17:

Attack= 0 19 19 0 2 10

بتشفير النص ينتج:

17 10 10 17 19 1 =rkkrtb

**ملاحظة** : يعتقد أن يوليوس قيصر هو أول من استخدم هذه الشيفرة بمفتاح 3 وتعد شيفرة ROT13 حالة خاصة منها عندما يكون مقدار الأزاحة 13 وهنا يمكن فك التشفير بدلا من طرح 13 بجمع 13 مرة أخرى .الآن سنتعرف كيف يتم كسر هذا النظام.

# مهاجمة القوة العمياء(*Brute - force attack*)

# هجوم القوة العمياء مبني على مبدأ بسيط يشرح بالمثال : أوسكار (المهاجم) لديه النص المشفر عن طريق التنصت على القناة و كان لديه جزء صغير من النص الأصلي, أوسكار يقوم بفك تشفير النص المشفر بكل مفتاح ممكن و أذا تلاءم النص المشفر بعد فكه مع النص غير المشفر يعرف أن هذا المفتاح . [[5]](#footnote-5) شكل (4)

**Definition Basic Exhaustive Key Search Or**

**Brute – force Attack**

***Let( X, Y ) denote the pair of plaintext and ciphertext, and let K = { k1, …. kk} be the key space of all possible keys ki. A brute – force attack noe checks for every ki€ K if :***

**dki(y) x**

***If the equality holds, a possible correct key is found; if not, proceed with the next key.***

**?**

**=**

**شكل (4) : تعريف شفرة مهاجمة القوة العمياء**

# ملاحظات عامــــة:

# 1- عملياً قد يكون الهجوم بالقوة العمياء أكثر تعقيدا، فأحيانا مفاتيح غير صحيحة قد تعطي نتائج أجابية خاطئة.

# 2- في جميع حالات التشفير بالمفتاح المتناظر، الهجوم بالقوة العمياء ممكن نظريا لكن عمليا إذا كان عدد احتمالات المفتاح كبير جدا قد يصعب تجريب جميع الاحتمالات.

# 3- كما لاحظنا بشفرة قيصر عدد احتمالات المفاتيح قليل جدا، لذا يمكن تجربة جميع الاحتمالات فهذا الهجوم عمليا ممكن عليها.

# 2.2 الفصل الثاني : *Affine Cipher*

# تعد مطورة عن التشفير بالأزاحة ويمكن تعريفها بالشكل اللآتي : [[6]](#footnote-6) شكل (5)

**Definition Affine Cipher**

***Let x,y,a,b∈Z26***

**Encryption: ek(x) = y ≡a ·x+bmod 26.**

**Decryption: dk(y) = x ≡f·(y−b) mod 26.**

**with the key: k = (a,b), which has the restriction: gcd(a,26) = 1.**

**شكل (5) : تعريف *Affine Cipher***

# ملاحظة : يمكن إيجادf بخوارزمية أقليدس.

# KEY SPACE =عدد احتمالات a\*عدد احتمالات b=12\*26=312

# نلاحظ أن عدد الاحتمالات أكبر من التشفير بالأزاحة لكن مع ذلك يمكن تطبيق الهجوم السابق و تجريبه.

# 3.2 الفصل الثالث : تعمية الاستبدال *Substitution Cipher*

# تعد من الطرق البسيطة في التشفير بالمفتاح المتناظر أيضا وقد استخدمت تاريخيا عدة مرات وهي تبديل كل حرف من الأبجدية بحرف آخر و هي الطريقة العامة و تعد كل الطرق السابقة حالات خاصة منها و هي تقوم على و ضع جدول واحد يربط كل حرف من النص الأصلي بحرف من النص المشفر بحيث لا يربط كل حرف بأكثر من حرف مثال : [[7]](#footnote-7)

|  |  |  |  |
| --- | --- | --- | --- |
| K = F | C = A | T = d | A = k |

# Attack = Kddkaf

# نفرض أننا اخترنا المفتاح بطريقة عشوائية بحيث لا يمكن للمهاجم معرفته ( علما أن المفتاح هنا هو الجدول الذي يربط كل حرف بحرف آخر وأنه لا يمكن ربط أكثر من حرف بحرف واحد ) يجب أن يمتلك المفتاح كل من بوب وأليس ( الشخصان اللذان يريدان التراسل) وأن يتم توزيعه بقناة آمنة بحيث لا يعرفه سواهما. مثال:

# Iqifccvqqrfbrdqvfllcqnardqcfjwhwzhrbnnbhcchwwhbsqvqbrehwqvhlq

# لا يبدو هناك أي معنى للنص المشفر مما يجعلنا نعتقد أن هذا النظام آمن أضافة ألى أن عدد احتمالات مفاتيح هذا النظام كبير جدا (26!) وهو عدد كبير جدا من الاحتمالات لا يمكن تجربتها حتى بالأجهزة الحديثة بأقل من عشر سنوات لذلك لا يمكن تطبيق المهاجمة بالقوة العمياء عليه لكن هناك طريقة أخرى لكسره..

# ملاحظة : هناك نوع من التشفير يعد حالة خاصة من الاستبدال وهو شفرة أتباش حيث يتم تبديل الحرف الأول باللغة بالأخير و الثاني بقبل الأخير وهكذا.

# 4.2 الفصل الرابع : *Letter Frequency Analysis* [[8]](#footnote-8)

# تعمل على تحليل البنية الداخلية للنص لاستبعاد أغلب احتمالات المفتاح ثم تجربة ما يتبقى على خلاف مهاجمة القوة العمياء التي كانت تعتبر النص المشفر غرفة مظلمة و لتطبيق هذه الطريقة يمكن إتباع هذه الخطوات :

# تحديد نسبة ظهور كل حرف من النص المشفر و مقارنتها مع نسبة ظهور الأحرف باللغة عامة بغية اكتشاف ما الذي يقابل هذه الأحرف بالنص الأصلي و غالبا ما تفيد في تحديد الأحرف التي تقابل الأحرف التي تتكرر كثيرا باللغة فمثلا بالنص السابق نلاحظ أن الحرف q قد ورد كثيرا مما يعني أنه يقابل أحد الأحرف التي ترد كثيرا كالحرف .E

# يمكن الاستفادة من أنه بالعديد من اللغات هناك أحرف غالبا ما تأتي مصحوبة بأحرف أخرى فمثلا بالانكليزية غالبا ما يأتي بعد الحرف Q الحرف U.

# و يمكن الاستفادة من الثلاثيات أن تركت الفراغات كand the أو من أدوات التعريف a an فأذا حاولنا كسر المثال السابق بهذه الطريقة سنحصل على :

**WE WILL MEET IN THE MIDDLE OF THE LIBRARY AT NOON**

# ALL ARRANGEMENTS ARE MADE

# ملاحظة : نقطة الضعف الأساسية للطرق السابقة هي أن كل حرف يعطي الحرف ذاته دائما بعد التشفير لذلك يمكن تطبيق الطريقة السابقة عليه.

# 5.2 الفصل الخامس : المبادئ الأساسية لعلم تحليل الشفرات

# *General Thoughts In Cryptanalysis*

# من الأمثلة السابقة لاحظنا عدة طرق لكسر التشفير وتعرفنا على التشفير التناظري بأمثلته التاريخية الآن سندرس بشكل أكثر دقة و تفصيلا عن ما هو كسر الشفرات.[[9]](#footnote-9) شكل (6)

**Cryptanalysis**

Social

Engineering

Classical

Cryptanalysis

Implementation

Attacks

**Brute - Force**

**Attack**

**Mathematical**

**Analysis**

**شكل (6) : مجالات علم تحليل الشفرات**

# 1. *Classical cryptanalysis* )) : علم الحصول على النص الأصلي plain text )) من النص المشفر (cipher text) و يقسم إلى :

# هجوم تحليلي ( *analytical attack*) : يدرس البنية الداخلية لطريقة التشفير وللنص المشفر.

# مهاجمة القوة العمياء( *brute - force attack* ) : يجرب كل الاحتمالات.

# 

# 2. ( *Implementation attacks* ) : تستخدم عندما يكون المهاجم على تماس مباشر مع الجهاز الذي يقوم بالتشفير حيث يقوم بملاحظة آلية العمل , النشاط الكهربائي .... لكن عندما تكون الاختراقات عبر الشابكة من النادر أن يتم استخدام هذا الأسلوب.

# 3. ( *Social engineering attacks*) : تعتمد على خداع المستخدم بدلا من نقاط الضعف بالخوارزمية.

# و نذكر أنه هناك نوعين من الهجمات :

# الأول : هجوم غير نشط ( *Passive Attacks* ) : و يقوم المخترق هنا بمراقبة تبادل البيانات محاولا فك التشفير الرسائل أو على الأقل معرفة طبيعة نظام التشفير لكن دون محاولة التأثير على عملية التبادل أو تخريب الرسائل المتبادلة.

# الثاني : هجوم نشط ( *Active Attacks* ) :و هنا يقوم المخترق بمراقبة تبادل البيانات و التأثير على عملية التبادل معتمدا على ثغرة معينة بالنظام بحيث أنه أما يكتشف المفتاح و يخل بخدمة التكاملية بإفساده الرسائل....

# بشكل عام يمكن القول أن الهجمات غير النشطة أكثر تطبيقا من الهجمات النشطة لكن الهجمات النشطة أكثر قوة. يوضح الشكل التالي نوعي الهجمات المشار إليها. شكل (7)

# P 3.jpg

**شكل (7) : تمثيل توضيحي للهجوم النشط والهجوم غير النشط**

# من الأمثلة السابقة نفكر بالموضوع الآتي كم عدد احتمالات المفاتيح بحيث يكون نظام التشفير آمنا من مهاجمة القوة العمياء[[10]](#footnote-10) ؟؟ الجدول الآتي يوضح إمكانيات الأجهزة حاليا و بناء عليه تكون الشفرة آمنة أذا كان عدد احتمالات المفتاح أكثر من 112 بت.

# Untitled.jpg

# كون الأجهزة في تطور مستمر لذا هذا ليس ثابتا ومن الصعب توقع كيف ستطور الأجهزة لتستطيع تجريب عدد أكبر من الاحتمالات بوقت أكثر لكن قانون مور *moore’s law* )) يقول أن إمكانيات الأجهزة تتضاعف كل 18 شهر تقريبا بنفس التكلفة و هو قانون تقريبي .

# وبما تحدثنا عن طرق الهجوم، تجدر الإشارة إلى وجود نظام تشفير آمن من كل الطرق السابقة على الرغم من اعتماده على مبدأ بسيط جداً وهو :

# الشفرة الآمنة *The One - Time Pad*

# تعد هذه الشفرة الأكثر أمانا على مدى التاريخ ،وهي تعد مستحيلة الكسر لكن في الوقت [[11]](#footnote-11)ذاته صعبة التنفيذ حيث أنها تحتاج لكتاب يحوي على أرقام مولدة بشكل عشوائي تستخدم لإزاحة أحرف النص (تطبيق شفرة الإزاحة بمفاتيح متعددة مولدة عشوائيا تتغير من حرف لحرف بالنص الأصلي)و لتطبيق ذلك يجب أن يكون عدد الأحرف العشوائية أكبر من عدد أحرف النص ،لفك التشفير نقوم بعكس عملية التشفير.

**الباب الثالث : موجز عن التشفير غير الكلاسيكي**

# سنتناول في هذا الباب التوقيع الإلكتروني ,التشفير بالمفتاح العام *Hash Functions* ,أمثلة عن البروتوكولات البسيطة , علما أننا قد ذكرنا بعض المفاهيم السابقة بالباب الأول لكن الآن سنتناولها بشكل أكثر تفصيلا و ما سندرسه الآن يعد أساسيات التشفير الحديث.

# 3. 1 الفصل الأول : التشفير بالمفتاح العام *Public Key Cryptography*

# خوارزميات التشفير المتناظر الحديثة كال *AES*وال *3DES* تتميز بسرعة و أمان كبيرين و هي مستخدمة بشكل واسع جدا لكن هناك محددات سنعرضها مهدت لظهور التشفير بالمفتاح غير المتناظر :[[12]](#footnote-12)

# 1- مشكلة توزيع المفاتيح : يجب أن يمتلك المفتاح كل من الطرفين مفتاح التشفير ليتم التبادل بشكل آمن و نذكر بأن القناة الأصلية غير آمنة أذا لا بد من وجود قناة آمنة في البداية فكما ذكرنا سابقا خوارزميات التشفير المتناظر تحتاج إلى حفظ المفتاح السري.

# 2- عدد المفاتيح الكبير جدا : حتى ولو قمنا بحل مشكلة توزيع المفاتيح ,تبقى لدينا مشكلة العدد الكبير من المفاتيح حيث أنكل زوج من المستخدمين يجب أن يكون عنده مفتاح خاص فإذا كان هناك n مستخدم سيكون هناك n\*n-1/2 مفتاح و كل فرد يجب أن يحتفظ ب n-1 مفتاح سري.

# 3- لا تحمي من الخداع من قبل أحد الطرفين : حيث أن كلا الطرفين لديهما نفس المفتاح فكلا الطرفين لهما نفس الصلاحيات لذلك لا يمكن الاعتماد على التشفير المتناظر في التطبيقات التي تطلب حماية ضد الجحود ،على سبيل المثال في تطبيقات التجارة الإلكترونية غالبا ما يكون مهما إثبات أن المشتري قام بإرسال طلب لشراء الشيء المعروض لكيلا يقوم المشتري بإنكار طلبه لشراء هذا الشيء المعروض.

# لحل تلك المشكلات قام كل من *Diffie*، *Hellman* و *Merkle*بإيجاد التشفير بالمفتاح غير المتناظر المبني على الفكرة: من غير الضروري أن يكون المفتاح المستخدم للتشفير سريا من الكافي أن يكون مفتاح فك التشفير سريا و مع المتلقي بحيث لا يقوم أحد بفك التشفير سوى الطرف المتلقي. أي يقوم بوب بنشر مفتاح التشفير ليراه الجميع و يحتفظ بمفتاح سري لفك التشفير يمكن تشبيه هذا النظام بنظام البريد القديم حيث يستطيع الجميع وضع الرسائل بالصندوق لكن لا يستطيع سو صاحب الصندوق الذي يملك مفتاح الصندوق فتحه ويعد المثال السابق بروتوكولا أساسيا لما يسمى *public-key encryption* . شكل (8)

# P 6-A.jpg

**شكل (8) : رسم توضيحي لفكرة التشفير بالمفتاح العام**

# 3. 2 الفصل الثاني : دالة التجزئة*Hash Function* [[13]](#footnote-13)

# هي دالة رياضية تأخذ الدخل اياً كان وتصدر خرجاً ذا حجم ثابت مهما اختلف حجم الدخل، وهذا الخرج يبقى ثابتاً إذا بقي الدخل ثابتاً من أهم الخصائص هذه الدالة هي عدم القدرة على استنتاج دخلها من خرجها ونعلم أنه إذا تغير الدخل فغالباً ما يتغير الخرج ونقوم بتوظيف هذه الخاصة والخواص السابقة لتحقيق مفهوم تكامل البيانات حيث نقوم بإدخال الملف إلى الدالة أولاً ثم إرسال الملف وخرج الدالة فيقوم المستقبل بإدخال الملف إلى الدالة ومقارنة خرج دالته مع خرج المرسل إليه، إذا تطابق الخرجان نقول أنه بنسبة كبيرة\_ تختلف حسب قوة الخوارزمية\_ أن الملف لم يتعرض لأي تعديل، أما إذا لم يتطابق الخرجان فنجزم أن الرسالة تعرضت لتعديل.

# ملاحظة (1) : هناك حالات يمكن أن يكون تغيير الدخل مع بقاء الخرج ثابتاً، وتقل هذه الحالات مع ازدياد قوة الخوارزمية وتسمى التصادمات

# ملاحظة (2) : يجب حماية كل من خرج دالة التجزئة للرسالة والرسالة لأن المهاجم قد يعدل عليهما بحيث يتلاءم خرج دالة التجزئة للرسالة الجديدة مع تعديله للخرج السابق. شكل (9)

# P 7.jpg

**شكل (9) : رسم توضيحي لفكرة دالة التجزئة**

# لتوضيح ما جاء ذكره، نأتي بالمثال الآتي :

# إذا كان لدينا دالة التجزئة ( ( Hالتي تعطي خرجاً قيمته 1 إذا أدخل إليه رسالة بعدد بتات فردياً ويعطي خرجاً قيمته 0 إذا كان عدد بتات الرسالة زوجياً وأردنا إرسال لرسالة فنقوم بإدخالها إلى الدالة ونرسلها هي وخرجها على قنات آمنة ليقوم الطرف الآخر بالتحقق من تكامل البيانات بمقارنة خرج الرسالة المرسلة إليه بعد فك تشفيرها بالخرج المرسل بعد فك تشفيره.نلاحظ وجود عدد كبير من التصادمات وهو الذي يكون أقل بالخوارزميات الحديثة.

# ومن أشهر خوارزميات دالات التجزئة الحديثة :

# MD5( *Message Digest 5*) : سميت كذلك لأنها خامس خوارزمية من النوع (Message Digest) تم كتابتها من قبل R.L Rivest، وقد ظهر أول إصدار من هذا النوع عام 1989 ، وظهر أحدث إصدار من هذا النوع عام 1991 .

# تأخذ خوارزمية ( MD5 ) الدخل أياً كان حجمه وتعطي خرجاً بحجم 128 بت .

# SHA1 ( *Secure Hash Algorithm 1*) : يجب أن يكون دخلها أقل من 642 بت ( 2 مليون GB ) وخرجها 160 بت دائماً، وبحال أراد أحدهم إرسال رسالة أطول من 642 بت ( مع العلم بأنها حالة نادرة جداً )، يتم تجزئة الرسالة إلى أجزاء أصغر، تم بها حل العديد من نقاط الضعف التي وجدت في MD5،لذلك هي أقوى من MD5 لكنها أصعب تطبيقاً على الحاسوب، لذا يتم استخدام الخوارزمية المناسبة للغرض، ومن الإصدارات الحديثة SHA256 / SHA512 ، تعطي هذه الإصدارات خرجاً حجمه 256 أو 512 بت

# الفصل الثالث: التوقيع الرقمي *Digital Signature*

# تعد التواقيع الرقمية من أهم الأدوات في التشفير، و لها تطبيقات كثيرة جدا تمتد من الشهادت الرقمية إلى التجارة الإلكترونية الآمنة حتى التوقيع القانوني للعقود وصولا للتحقق من مصدر تحديثات الرنامج ، فهي تقوم بالكثير من الوظائف التي تقوم بها التواقيع العادية فهي تستخدم للمصداقية و منع الجحود .

# نعرف التوقيع الالكتروني لشخص ما على ملف ما على أنه مجموعة من البيانات بحيث إذا امتلك [[14]](#footnote-14)شخص ما كل من الملف و التوقيع يمكن أن يتأكد من و أن يثبت قانونيا إذا احتاج أن صاحب التوقيع هو الذي أرسل الملف .

# إن خوارزمية التوقيع الإلكتروني تقسم إلى عمليتين أساسيتين كما يلي : [[15]](#footnote-15)

# عملية توليد التوقيع الإلكتروني ( *Signature Generation Process* ) : وفيها يتم إدخال الملف إلى دالة التجزئة ومن ثم يقوم الموقع باستخدام مفتاحه الخاص على خارج الدالة للملف ليولد التوقيع الالكتروني، وفي النهاية يعطي كل من الملف و التوقيع الإلكتروني إلى المتحقق. ويجب أن يكون صاحب التوقيع هو المالك الوحيد للمفتاح الخاص

# عملية التحقق من التوقيع (*Verifier Process Signature* ) :يقوم المتحقق بإدخال الملف المرسل إليه بدالة التجزئة ذاتها التي استخدمها الموقع و مقارنة خارج التابع للملف مع التوقيع الإلكتروني بعد استخدام المفتاح العام عليه.

تتطلب عملية التحقق من التوقيع الرقمي التأكد من أن المفتاح العام المستخدم للتحقق يعود فعلاً للطرف الذي يزعم أنه صاحب التوقيع من جهة، وأن هذا المفتاح العام صحيح رياضياً من جهة أخرى.من خلال التحقق من هذه الأمور يتأكد الطرف المتحقق من أن التوقيع الرقمي صالح ( وأن صاحب زوج المفاتيح هو فعلاً من قام بالتوقيع ).

لذا فإن عملية التحقق من التوقيع الرقمي تقسم إلى:

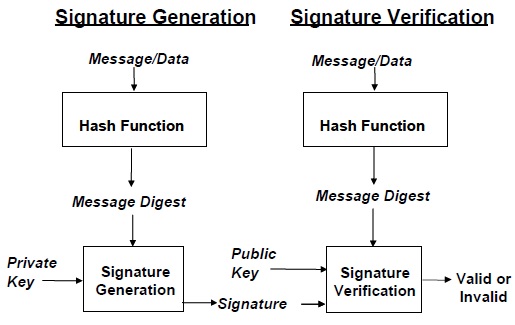
* **التحقق الرياضي من المفاتيح**.
* **التأكدات الضرورية ( من صاحب المفتاح العام )**.

نعرض هنا لماذا هذه التأكدات ضرورية :

1- إذا كان الطرف المتحقق من التوقيع لا يملك وسائل للتأكد من أن الطرف الموقع هو فعلاً صاحب المفتاح العام المستخدم في التوقيع، فإنه عندئذ يمكن لأي شخص بحوزته زوج من المفاتيح أن يوقع أي رسالة بمفتاحه الخاص زاعماً أنه أي شخص آخر، ويحدث عندئذ التحقق الصحيح عند الطرف المتحقق باعتباره لا يملك الوسائل المناسبة للتحقق من أن المفتاح العام يعود لذلك الشخص.

( وهذا مثل على نظامحقق مبدأ التكاملية ولم يحقق المصادقة ).

2 – إذا كان المفتاح العام غير صالح رياضياً فإن عملية التحقق غير مفيدة أبداً، ( يمكن أن يكون صاحب المفتاح ليس هو الشخص الوحيد القادر على توقيع رسائل بهذا المفتاح ). أي أنه توجد مفاتيح أخرى تؤدي نفس الغرض بسبب عدم تحقيق المفتاح للشروط الرياضية اللازمة ).

****

**شكل (10) : رسم توضيحي لفكرة التوقيع الرقمي**

**الباب الرابع : النتائج العامة للبحث**

أوردنا في هذه الحلقة المفاهيم الأساسية لعلم التشفير و حاولنا الإجابة عن عدة أسئلة،و أخيرا عرضنا بعض التطبيقات الحديثة له و من النتائج الهامة التي يمكن استنتاجها هي سمات نظام التشفير الناجح :

1. أن تكون مهاجمة القوة العمياء هي أسهل هجوم يمكن تطبيقه على النظام .
2. أن يكون عدد المفاتيح كافيا كما شرحنا في الباب الثاني الفصل الخامس.
3. أن أن يكون آمنا من social engineering, implementation attack ,analytical attack.
4. أن يحقق أهداف التشفير (التكاملية، المصداقية، عدم الجحود، الخصوصية) .
5. لاحظنا أن علم كسر الشفرات كان السبب لتطور علم التشفير عبر التاريخ لذلك يجب على نظام التشفير القوي أن يعرض كاملا دون إخفاء تفاصيله على العامة و على مختصين بالتشفير لأن إخفاء الخوارزمية يؤدي إلى عدم تجريبها مع إمكانية قيام المهاجم باكتشافها.

كما لاحظنا أيضاً أن تصميم أنظمة الأمان أكثر حساسية من تصميمات البرمجيات العادية لأنه تحت ظروف الاستعمال العادية فإن النظام الخالي من الأخطاء بنسبة 99.99% نادرا ما يقع في الخطأ أما في أنظمة الأمان فإن الخطأ بنسبة 0.01% يمكن أن يتم استغلاله فيتحول بذلك الخطأ إلى 100%. الشكل التالي يوضح ما سبق :

|  |  |
| --- | --- |
| Untitled1.jpg | Untitled2.png |

**شكل (11) : شكل توضيحي للفرق بين أنظمة الأمان و البرمجيات العادية**

|  |  |  |
| --- | --- | --- |
| **رقم**  **الشكل** | **قائمة الأشكال والجداول** | **رقم الصفحة** |
| **شكل (1)** | **مجالات علم التشفير ..........................................** | **3** |
| **شكل (2)** | **رسم توضيحي لآلية التشفير بالمفتاح المتناظر ................** | **5** |
| **شكل (3)** | **تعريف شيفرة التشفير بالإزاحة ................................** | **7** |
| **شكل (4)** | **تعريف شيفرة مهاجمة القوة العمياء ...........................** | **8** |
| **شكل (5)** | **تعريف شيفرة الــ : *Affine Cipher* ................................** | **9** |
| **شكل (6)** | **مجالات علم تحليل الشفرات ...................................** | **11** |
| **شكل (7)** | **تمثيل توضيحي للهجوم النشط والهجوم غير النشط ............** | **12** |
| **شكل (8)** | **تمثيل توضيحي لفكرة التشفير بالمفتاح العام ...................** | **15** |
| **شكل (9)** | **تمثيل توضيحي لفكرة دالة التجزئة .............................** | **16** |
| **شكل (10)** | **تمثيل توضيحي لفكرة التوقيع الرقمي ..........................** | **18** |
| **شكل (11)** | **شكل توضيحي للفرق بين أنظمة الأمان و البرمجيات العادية ..** | **20** |

|  |  |  |
| --- | --- | --- |
|  | **قائمة مراجع البحث** |  |
| **1. وجدي عصام عبد الرحمن \_ 2007 :** مقدمة في التشفير بالطرق الكلاسيكية (نسخة مبدئية). | | |
| **2 .** ***Christof Paar& Jan Pelzl \_ 2010 :*** Understanding Cryptography \_ Heidelberg, Dordrecht, London, New York.. | | |
| **3 . John Edward Silva\_2003:**An Overview of Cryptographic Hash Functions and Their Uses\_SANS Institute,p.1\_4. | | |
| **4 . leslie lamport**\_1979 : Constructing Digital Signatures From A One Way Function,Microsoft.P.1 | | |
| **6 . gary locke , 2009:** Digital Signature Standard (DSS)\_National Institute Of Standards and technology.USA.p.9\_11 | | |

1. **. وجدي عصام عبد الرحمن \_ 2007 :** مقدمة في التشفير بالطرق الكلاسيكية (نسخة مبدئية)ص. 23. [↑](#footnote-ref-1)
2. **.** ***Christof Paar& Jan Pelzl \_ 2010 :*** Understanding Cryptography \_ Heidelberg, Dordrecht, London, New York. P.4\_5 [↑](#footnote-ref-2)
3. ***Christof Paar& Jan Pelzl \_ 2010 :*** Understanding Cryptography \_ Heidelberg, Dordrecht, London, New York. P.3 [↑](#footnote-ref-3)
4. **.*Christof Paar& Jan Pelzl \_ 2010 :*** Understanding Cryptography \_ Heidelberg, Dordrecht, London, New York. P. 17-18. [↑](#footnote-ref-4)
5. **. *Christof Paar& Jan Pelzl \_ 2010 :*** Understanding Cryptography \_ Heidelberg, Dordrecht, London, New York. P. 7. [↑](#footnote-ref-5)
6. **. *Christof Paar& Jan Pelzl \_ 2010 :*** Understanding Cryptography \_ Heidelberg, Dordrecht, London, New York. P. 19 – 20. [↑](#footnote-ref-6)
7. **. *Christof Paar& Jan Pelzl \_ 2010 :*** Understanding Cryptography \_ Heidelberg, Dordrecht, London, New York. P. 6 – 7. [↑](#footnote-ref-7)
8. **. *Christof Paar& Jan Pelzl \_ 2010 :*** Understanding Cryptography \_ Heidelberg, Dordrecht, London, New York. P.8 [↑](#footnote-ref-8)
9. **. *Christof Paar& Jan Pelzl \_ 2010 :*** Understanding Cryptography \_ Heidelberg, Dordrecht, London, New York. P.10 [↑](#footnote-ref-9)
10. ***Christof Paar& Jan Pelzl \_ 2010 :*** Understanding Cryptography \_ Heidelberg, Dordrecht, London, New York. P.12 [↑](#footnote-ref-10)
11. **. وجدي عصام عبد الرحمن \_ 2007:** مقدمة في التشفير بالطرق الكلاسيكية (نسخة مبدئية)61 [↑](#footnote-ref-11)
12. **. *Christof Paar& Jan Pelzl \_ 2010 :*** Understanding Cryptography \_ Heidelberg, Dordrecht, London, New York. P.151\_152 [↑](#footnote-ref-12)
13. **. John Edward Silva\_2003:**An Overview of Cryptographic Hash Functions and Their Uses\_SANS Institute,p.1\_4. [↑](#footnote-ref-13)
14. **. leslie lamport**\_1979 : Constructing Digital Signatures From A One Way Function,Microsoft.P.1 [↑](#footnote-ref-14)
15. **. gary locke , 2009:** Digital Signature Standard (DSS)\_National Institute Of Standards and technology.USA.p.9\_11 [↑](#footnote-ref-15)