

موقع توعرب التعليمي

[www.arabia2.com/vb](https://www.arabia2.com/vb)

*العامة للمناهج األمن السيرباني اإلدارة*

0



*اإلدارة العامة للمناهج*

*التدريب اجملتمعي*

*احلقيبة التدريبية*

*األمن السيرباني*

*(بنني* & *بنات)*

وعلى آله

بن عبد اهلل

*مقدمة*

والصالة والسالم على من ال نيب بعده، حممد

احلمد هلل وحده

وصحبه، وبعد:

املؤسسة العامة للتدريب التقين واملهين ومتاشيا مع حتقيق رؤية التحول رأت أن تتقدم خدمات تدريبية بعض احلقائب التدريبية من منطلق حرص الوطين واملساهمة يف اخلدمة اجملتمعية

تدريب يف

ساعة

بشكل مُبسط يف حمتوى تدرييب تقدميه يف دورات قصرية ال تتجاوز 16

جلميع شرائح اجملتمع الراغبني يف اكتساب مهارات يف أحد التخصصات اليت األسبوع، تُقدم

تهمهم يف حياتهم اليومية.

*وتتناول هذه احلقيبة التدريبية* ***" األمن السيرباني "*** *ملتدربي برامج التدريب اجملتمعي*

حيوية تتناول الثقافة املهنية واكتساب املهارات األولية هلذا الربنامج التدرييب. موضوعات

واإلدارة العامة للمناهج وهي تضع بني يديك هذه احلقيبة التدريبية تأمل من اهلل عز وجلً

تسهم بالشكل مباشر يف تأصيل املهارات الضرورية الالزمة، بأسلوب مبسط خيلو من أن

بالتطبيقات واألشكال اليت تدعم عملية اكتساب هذه املهارات. على إعدادها واملستفيدين منها ملا حيبه ويرضاه، إنه مسيع التعقيد، مدعم واهلل نسأل أن يوفق القائمني

جميب الدعاء.

اإلدارة العامة للمناهج

*الفهـــرس*

|  |  |
| --- | --- |
| *رقم الصفحة* | *املوضـــــوع* |
| 1 | *مقدمة* |
| 2 | *الفهرس* |
| 3 | *متهيد* |
| 4 | *مقدمة التشفري والرتميز* |
| 4 | *كيف نقوم بعملية التشفري؟* |
| 11 | *علم التشفري احلديث* |
| 14 | *األمن اإللكرتوني* |
| 16 | *التحكم بالوصول* |
| 18 | *حاالت البيانات* |
| 20 | *التكنولوجيات* |
| 21 | *التحكم يف الوصول* |
| 22 | *املفاهيم* |
| 26 | *التصديق* |
| 33 | *االقسام واالهداف* |
| 34 | *الربنامج الضار والتعليمة الربجمية الضارة* |
| 45 | *اخلداع* |
| 47 | *اهلجمات* |
| 55 | *احلماية* |
| 55 | *تأمني الشبكة* |
| 57 | *التوعية بشأن أمن املعلومات* |
| 57 | *التشفري* |
| 66 | *املعادالت الصعبة* |
| 70 | *التوقيعات الرقمية والشهادات* |
| 70 | *التوقيعات والقانون* |
| 73 | *بروتوكول طبقة الوصل اآلمنة/ بروتوكول* |

*متهيد*

اهلدف العام من احلقيبة:

هذا الربنامج إىل إكساااااااااااب املتدرب املهارات واملعلومات األساااااااااااسااااااااااية يف األمن يهدف

السيرباني.

تعريف باحلقيبة: احلقيبة املفاهيم األولية األساااااسااااية عن االمن الساااايرباني، حيث ساااايتمكن السااايرباني، ما املقصا**ا**ود بالتشاافري ، الكتابة املخفية، تصاااميم تقدم هذه املتدرب من التعرف على األمن

األكواد )التشفري(، باإلضافة إىل فك األكواد )حتليل الشفرات.(

الوقت املتوقع إلمتام التدريب على مهارات هذه احلقيبة التدريبية:

يتم التدريب على مهارات هذه احلقيبة يف 16 ساعة تدريبية، موزعة كالتالي:

ساعات تدريبية 4

ساعات تدريبية 4

ساعات تدريبية 4

ساعات تدريبية 4

نظرية األمن اإللكرتوني

األكواد الضارة تأمني الشبكة علم التشفري

*الوحدة* *:*1

*الوحدة* *:*2

*الوحدة* *:*3

*الوحدة* *:*4

*األهداف التفصيلية للحقيبة:*

من املتوقع يف نهاية هذه احلقيبة التدريبية أن يتقن املتدرب ما يلي:

1 . التعرف على بيئة عمل احلاسوب الشخصي املعاصر.

2 . التعرف على ختزين كلمة السر.

3 . التعرف على تقنيات اهلندسة االجتماعية.

4 . التعرف على عمليات الغش وكيفية متيزها.

5 . كيفية جتنب أن تكون ضحية هجمات على شبكة االنرتنت.

6 . التعرف على الفريوسات وأخطار شبكة االنرتنت.

موجز قصري عن التشفري الرتميز

ما املقصود بالتشفري؟

 موسوعة بريتانيكا:

ممارسة تشفري وفك رموز الرسائل يف الكود السري جلعلها غري مفهومة  "التشفري:

للجميع باستثناء املستقبِل املقصود."

 "*الكتابة املخفية*"

 استخدم حتى وقت قريب كأداة عسكرية

 وكأي تقنية عسكرية أخرى: فقد تغري مبرور الزمن

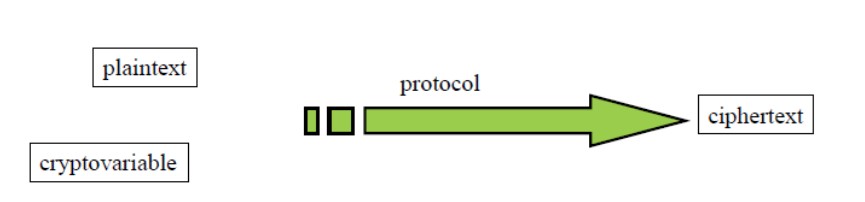
 جانيب التشفري:

 تصميم األكواد (التشفري(

 فك األكواد (حتليل الشفرات(

 غريت احلواسيب كال اجلانبني

# كيف نقوم بعملية الرتميز؟

الربوتوكول أو اخلطة: طرق الرتميز . للتشفري أو املفتاح: معلومات سرية قابل

باملفتاح املتناظر وفك التشفري هو نفس الشيء يف احلضارة السومرية التشفري استخدام التشفري

• 3500*قبل امليالد: السومريني*



• الكتابة املسمارية

استخدام التشفري يف احلضارة املصرية

• 1900*قبل امليالد: مصر*

• أول من عرف استخدام التشفري

استخدام التشفري يف احلضارة اليونانية

• 486*قبل امليالد: اليونان*

*.*–Σκυτάλη skee tah lee •



استخدام التشفري يف احلضارة الرومانية

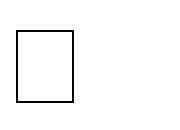
• 50-60 *قبل امليالد: يوليوس قيصر*

شفرة االستبدال

• حتويل احلروف مبواضعx:



F,

: E.g. X = 3: A D, B E, C

• *مثال*...



• ما هي نقاط الضعف؟

• *حتليل التكرار* 1000*( م*)

• 1466*ليون أربنتيين: قرص الشفرة*

• استخدمت حتى القرن السادس عشر

مثال شفرة قيصر

• الربوتوكول: حتويل كل حرف بنفس املقدار .

• القابل للتشفري: مقدار التحويل

Veni, vidi, vici Foxs, fsns, fsms

• فك التشفري: فك التحويل بنفس املقدار

• احلالة األوىل: يف حال عدم معرفتنا الربوتوكول

• مشكالت عويصة عند حتليل الشفرات

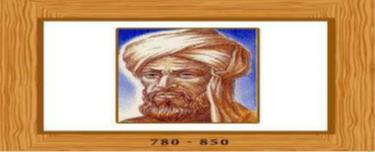
• احلالة الثانية: يف حال معرفتنا بالربوتوكول



• حنتاج لتخمني إمكانية فك الشفرات

• يوجد 26 احتمال فقط

• حممد بن موسى اخلوارزمي



• علم فلك ورياضيات مسلم ومنجم وعامل جغرافيا.

• طور مفهوم اخلوارزميات يف

• علم الرياضيات.

• يعترب علم اجلرب الذي وضع أساسه اخلوارزمي أساس وحجر األساس هذا العلم

• "*ندين للخوارزمي باخرتاعه علم اجلرب*

• مقتبس من كتاب "املختصر يف حساب اجلرب واملقابلة"

**•** الكندي



• علم التشفري احلديث الذي نشأ بني العرب، وكانوا أول من يوثقون طرق التشفري

بشكل منهجي.



• الكندي: عامل رياضيات مسلم، وُلد حوالي عام 800م اخرتع تقنية تواتر احلروف

لفك شفرات االستبدال احادية األجبدية

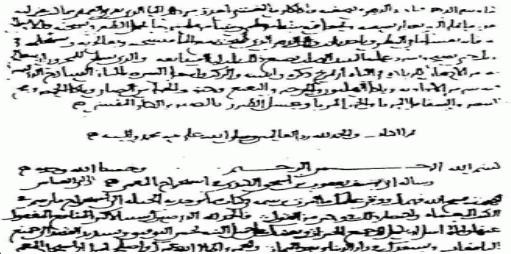
• أثبت أهمية التقدم ال 1ي أحرزه يف هذا العلم حتى احلرب العاملية الثانية.

رساالاة فاي اساتاخاراج الاماعامّاى

الكندي كتاباً يف علم التشفري بعنوان "خمطوطة فك رسائل التشفري" والذب • ألف

أول التقنيات التشفريية، وتشمل بعض الشفرات متعددة األجبدية وتصنيف الرتاكيب وأكثرهم أهمية، وضع أول اوصافه عن تواتر وصفها بأن تكون التشفري وعلم الصوتيات العربي وعلم

احلروف.



طرق التشفري، وحتليل شفرات بعض الشفرات، والتحليل االحصائي للحروف • غطى ايضاً

وبعض تركيبات احلروف يف اللغة العربية.

أمحد القلقشندي

 *تاريخ امليالد:* 1418*-*1355

 ألف كتاب صبح األعشى

 موسوعة تتكون من 14 جزء ويشتمل على قسم يف التشفري.

هذه املعلومة من العامل ابن الدريهم، الذي عاش يف فرتة من عام 1312وحتى  مت استقاء

1361 ولكن فقدت مؤلفاته عن علم التشفري.



شفرة فجنري العامل بليز دو فجنري (املولود عام 1587 م ( متعددة األجبدية: العالقة واحد إىل متعدد شيفرة

مثال.

*الكلمة املشفرة*lamp :

*كلمة السر*ubc :

*النص املشفر*fboj :

قام بفك الشفرة العامل بابيج وكاسيسكي 1863(م(

اكتشاف طول كلمة السر الرسالة إىل قطع استبدال مشفرة استخدام تواتر احلروف حللها تقسيم

## :1845

شفرة مورس إشارة مشفرة عرض

حاالت(التشغيل واإلطفاء) املكونة من 5 رموز

ADFGVX

:1918

شفرةADFGVX اجليش األملاني يف احلرب العاملية األوىل استخدمها



## 



















مورس



















• آلة إجنما

• نظام تشفري استخدمته أملانيا يف احلرب العاملية الثانية.

• الفكرة: تعديل اخلطابات

• قرص تشويش يستخدم لعملية التبديل

• يقوم بالدوران بعد كل حرف، يستخدم الكثري من عمليات التبديل

• عمليات تبديل إضافية، باستخدام لوحة املفاتيح

• آالن تورنغ: لوحة مفاتيح حمولة

• متكن الربيطانيون من قراءة الرموز

• قسم تكنولوجيا املعلومات واالتصاالت

• املتحدثون بشفرة نافاجو

• استخدمها األمريكان يف حرب احمليط اهلادئ أثناء احلرب العاملية الثانية.

• وكان لدى كل فصيلة واحداً من شعب نافاجو

• وبالرغم من كشف النظام، إال أن اليابانيون مل يستطيعوا فك الشفرات

• مثل لوحة املرة الواحدة: يعد السر احملبك مسبقاً، لغة كاملة

• رمبا بال ميكن استخدامها يف الوقت احلالي



علم التشفري احلديث



• 1949*شانون*

• نظرية االتصال لنظم األسرار

• خوارزمية رياضية حتول النص اجملرد إىل نص مشفر، ألغراض أمنية

• افرتاض أن األعداء قاموا بكشف الربوتوكول

• ويكون املفتاح وحده سر

• التشفري، استخدام أجهزة احلاسوب لتحليل الشفرات

• متاحة للجميع، السماح للجميع مبحاولة فك الشفرة

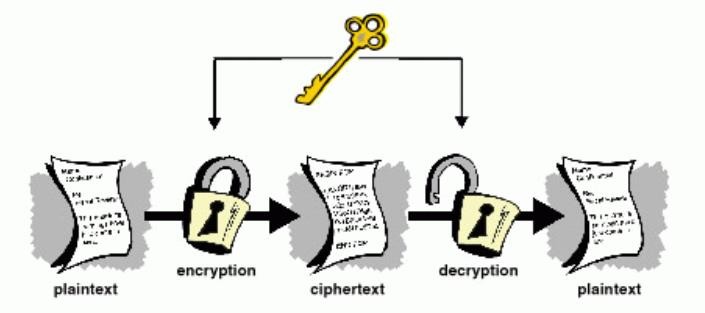
• دائما يفشل التصميم املغلق (اهلواتف النقالة)

• املصطلحات األساسية واملسائل املوضحة

• دراسة حالة: الفريوس املنتقل ستوكسنت

# 



***تشفري باملفتاح املتناظر***

• خوارزمية واحدة قوية

• جيب أن يظل مفتاحني سراً

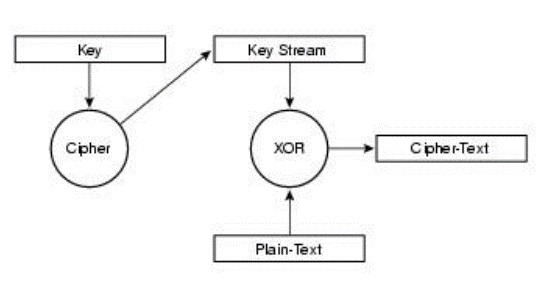
• تشفري تدفقي

• سلسلة املفتاح. عمليةxor

• التغذية املرتدة اخلطية

• التغذية املرتدة غري اخلطية

• مولد ستوب أند جو

• املولد املتقلص

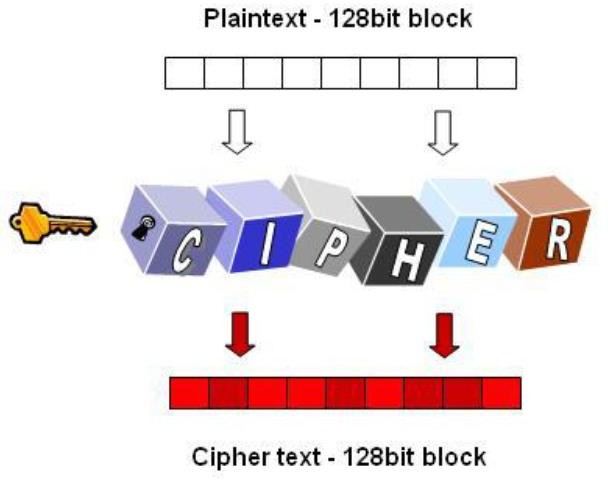
 التشفري الكتلي

 شفرة فيستيل ثابتة الطول

 دالة اجلولة

 معيار تشفري البيانات

 مقاييس التشفري املتقدمة



 حتليل الشفرات واملهتمون بالتشفري

 هجوم النص املشفر. نوعان

 احملرتف واهلاوي

 نقاط الضعف

 هجوم عنيف

 حتليل الشفرات اخلطية

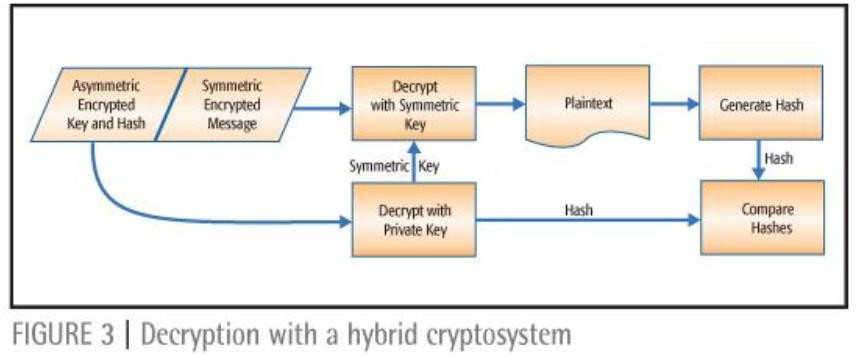
 حتليل التعمية التفاضلي

 التشفري املتناظر وغري املتناظر

 التشفري املختلط

 خصوصية جيدة جداً

 خصوصية جيدة جدًا مفتوحة



 سجالت الدخول املشفرة

 بروتوكول النقل اآلمن

 تسجيل دخولR

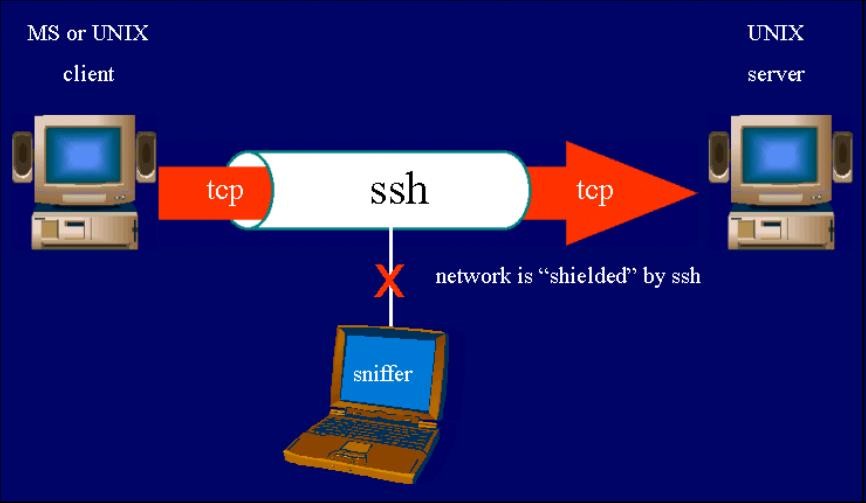
 كريبريوس

 طوابع زمنية

 مفتاح جلسة العمل

 مفتاح سري

- جتزئة من ناحية واحدة





- دراسة حالة:

- فريوس متنقل ستوكسنت

- ستوكسنت

- فريوس متنقل ضار، واليت ظهرت ألول مرة عام .2010

- وظل يف مرحلة التطور منذ عام 2005 على األقل

- يستهدف أنظمة سكادا -عناصر التحكم املنطقية القابلة للربجمة

- ُيعتقد انها املسؤولة عن التلف الفعلي لربنامج إيران النووي.

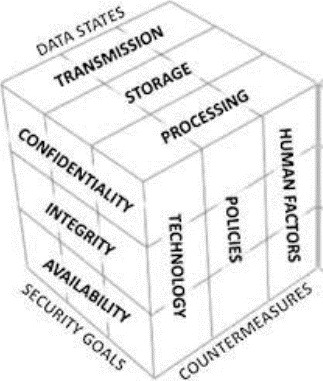
- شاهد مقطع الفيديو وناقش.

- اليوم األول: نظرية األمن اإللكرتوني

- ورشة عمل للتوعية بشأن أمن املعلومات، خريف 2018

- البعد الثالث لألمن اإللكرتوني

- مكعب األمن اإللكرتوني



األهداف االمنية

البعد األول مبكعب االمن اإللكرتوني األهداف حلماية العامل اإللكرتوني. كما  ُيعرف

أهداف البعد األول املبادئ األساسية لعامل األمن اإللكرتوني. ُتحدد

 وهناك ثالثة مبادئ أال وهي السرية، والتكامل والتوفر.

املبادئ الرتكيز ملتخصصي األمن اإللكرتوني وتتيح هلم فرض وضع أولويات  توفر هذه

إلجراءاتهم جتاه محاية العامل اإللكرتوني.

 استخدم االختصار CIA لتتذكر الثالثة مبادئ.

 السرية



السرية اإلفصاح عن املعلومات واملوارد والعمليات لغري املسؤولني. وهناك تعبري آخر  متنع

يستخدم بدالً من السرية أال وهو اخلصوصية.

املؤسسات إىل تدريب موظفيها على أفضل ممارسات محاية املعلومات احلساسة  حتتاج

حلماية أنفسهم ومؤسساتهم من اهلجوم.

 تستخدم هذه األساليب لضمان السرية مبا يف ذلك تشفري البيانات، واملصادقة والتحكم

بالوصول.

 خصوصية البيانات

جتمع املؤسسات جمموعة كبرية من البيانات وتكون الكثري من هذه البيانات غري 

حساسة ألنها متوفرة للجميع، مثل األمساء وأرقام اهلاتف.

الرغم من أن البيانات األخرى املُجمعة حساسة. وتعترب املعلومات احلساسة بيانات  فعلى

مؤمنة من الوصول غري املصرح حلماية الفرد أو املؤسسة.

كالً من السرية واخلصوصية، ولكن من وجهة نظر قانونية، فإنهم يعنوا شيئني  وتبدو

خمتلفني.

 فمعظم البيانات خاصة، ولكن ليس مجيعها سري.

 كما حتتوي املعلومات السرية على حالة خاص.

 وتتعلق اخلصوصية باستخدام البيانات املالئمة.

**التحكم بالوصول** خمططات احلماية اليت متنع الوصول غري املرخص جلهاز الكمبيوتر، أو قاعدة ُيعرف عدد من

البيانات، أو موارد البيانات األخرى. وتشرتك مبادئ AAA الثالثة يف خدمات التأمني:

***املصادقة*** *تتحقق من هوية املستخدم ملنع الوصول غري ا ُملرخص*.-

**التخويل** ُتحدد املوارد اليت يستطيع املستخدمني الوصول هلا باإلضافة إىل العمليات- **خدمات**

يستطيع املستخدمني القيام بها. ويستطيع التخويل التحكم عند وصول املستخدم إىل اليت

مورد ُمحدد.

**احملاسبة** تتعقب ما يفعله املستخدمون مبا يف ذلك ما يصلون له وكم من الوقت يستغرقون-

أثناء االطالع على املوارد والتغيريات اليت يقومون بها.



# التكامل

تكامل البيانات: التكامل هو الدقة، واالتساق، وموثوقية البيانات أثناء دورة احلياة - مبدأ

احلالية.

وهناك تعبري آخر يستخدم بدالً من التكامل أال وهو اجلودة. -

تستخدم األساليب لضمان تكامل البيانات مبا يف ذلك التجزئة، والتحقق من صحة -

البيانات، والتحقق من اتساق البيانات، وأدوات التحكم بالوصول.

o احلاجة إىل تكامل البيانات.

يعترب محاية تكامل البيانات حتدي ثابت مبعظم املؤسسات. -

o التحقق من التكامل

هو أسلوب لقياس اتساق جمموعة البيانات.

# التوفر

توفر البيانات مبدأ مستخدم لوصف احلاجة للحفاظ على توفر أنظمة املعلومات - يعترب

واخلدمات جبميع األوقات.

اهلجمات عرب اإلنرتنت وفشل االنظمة منع الوصول ألنظمة املعلومات واخلدمات. - تستطيع

تستخدم األساليب لضمان التوفر مبا يف ذلك تكرار النظام، ونسخ النظام االحتياطية، -

النظام املتزايدة، وصيانة املعدات، وأنظمة التشغيل والربامج احلديثة، واخلطط ومرونة

املناسبة السرتداد ما ضاع من معلومات املفاجئ بسرعة.

االنظمة عالية التوفر على ثالثة مبادئ للتصميم: استثناء نقاط اخلطأ الفردية، - وحتتوي

وتوفري النقل اآلمن، والكشف عن األخطاء اليت قد حتدث.

# عدم اإلنكار

- لن تستطع املؤسسة نفي (إنكار) اإلجراءات السابقة

يعترب عدم اإلنكار هو القدرة على إثبات أو عدم إثبات أن شيء حدث مثل املعامالت - حيث

أو ضم التوقيعات باتفاقية قانونية. بالعمليات القانونية وذلك ملنع الكيانات من االدعاء بعدم املوافقة على املالية - وهلذا األمر جذور

شيء أو توقيع مستند.



# حاالت البيانات

- العامل اإللكرتوني هو عامل البيانات.

- ُيركز متخصصو التأمني اإللكرتوني على محاية البيانات.

البعد الثاني من مكعب التأمني اإللكرتوني على مشكالت محاية مجيع حاالت - وُيركز

البيانات ضمن العامل اإللكرتوني.

- وتتضمن البيانات ثالثة حاالت حمتملة:

1 ) البيانات احملتجزة أو املُخزنة

2 ) البيانات املنقولة

3 ) البيانات قيد املعاجلة

# بيانات ثابتة

البيانات الثابتة أن نوع من جهاز التخزين حيتفظ بالبيانات عندما تستخدمها العملية. - تعين

- البيانات اليت مت ختذينها تشري إىل البيانات الثابتة.

جلهاز التخزين ان يكون حملي (على جهاز حاسوبي) أو مركزي (على الشبكة). - ميكن

- أجهزة التخزين املرتبط بالشبكات

- مصفوفة التعدد لألقراص املستقلة

- التخزين الشبكي

- شبكة منطقة النظام

# بيانات متنقلة

- يتضمن نقل البيانات إرسال املعلومات من جهاز إىل األخر.

- هناك العديد من الوسائل لنقل املعلومات بني األجهزة واليت تضمن علي:

البيانات عن طريق الساعي -تستخدم الوسائط القابلة لإلزالة لتحريك البيانات من - نقل

حاسبو إىل األخر التلقائية -تستخدم الكابالت لنقل املعلومات - الشبكات

- الشبكات الالسلكية-تستخدم املوجات الكهرومغناطيسية لنقل البيانات.

- محاية البيانات املنقولة أحد أكثر الوظائف أمن االنرتنت صعوبة.



وأكرب الصعوبات هي:

محاية سرية البيانات نزاهة البيانات - البيانات - محاية - محاية توفر

# بيانات قيد املعاجلة

- احلالة الثالثة من البيانات هي البيانات قيد املعاجلة.

هذا يشري إىل البيانات خالل املدخالت األولية أو التعديل أو احلوسبة او املدخالت. -

- تبدأ محاية نزاهة البيانات من املدخالت األولية للبيانات.

جتميع البيانات مثل إدخال البيانات يدوياً ومناذج املسح الضوئي ورفع البيانات - وسائل

والبيانات اجملمعة من أدوات االستشعار، يشكل تهديدات حمتملة إىل نزاهة البيانات.

تعديل البيانات إىل أي تغري يف البيانات األصلية مثل تعديل املستخدمني للبيانات يدوياً - يشري

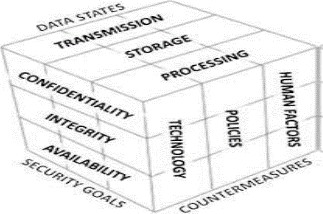
ومعاجلة البيانات وتغري البيانات وفشل املعدات املتسببة يف تعديل البيانات

ترميز/ فك الرتميز ضغط/فك الضغط - / فك التشفري - - التشفري

# اإلجراءات املضادة (عوامل احلماية(

البعد الثالث مبكعب االمن اإللكرتوني حيدد أنواع السلطات املستخدمة حلماية - ُيعرف

العامل اإللكرتوني.

- حيدد مكعب السحر االنواع الثالثة من السلطات:

## -

- التكنولوجيات -األجهزة واملنتجات متاحة حلماية أنظمة املعلومات وحتاشي جمرمي

األنرتنت.



واملمارسات -اإلجراءات واإلرشادات اليت متكن مواطنني عامل االنرتنت من - السياسات

البقاء يف حالة من األمن واتباع املمارسات احلسنة

األشخاص -الذين على دراية ووعي بعاملهم واملخاطر اليت تهدد عاملهم. -

# التكنولوجيات

**- *تكنولوجيات احلماية املستندة إىل الربامج***

- مكافحة الفريوسات وجدار احلماية ومكافحة الربامج الضارة وتصفية احملتوى

# - تكنولوجيات احلماية املستندة إىل األجهزة

أنظمة الكشف عن حماوالت التدخل وأنظمة منع حماوالت التدخل وتصفية احملتوى -

# - تكنولوجيات احلماية املستندة إىل الشبكة

- الشبكة اخلاصة الظاهرية التحكم يف الدخول إىل شبكة نقطة الوصول الالسلكي - - أمن

# - تكنولوجيات احلماية املستندة إىل السحابة

الربامج كخدمة األساسية كخدمة - األمان الظاهرية - البنية - أجهزة

# التعليم والتدريب يف جمال أمن األنرتنت

- يعد برنامج التوعية باألمن يف غاية االهمية للمؤسسات.

- قد ال يقصد املوظف الضرر ولكنه جيهل اإلجراءات الواجب تنفيذها .

- هناك العديد من الطرق لتنفيذ برنامج تدرييب رمسي:

برنامج لرفع الوعي يف جمال االمن كجزء من عملية اإلحلاق الفعلي بالعمل. - إقامة

- ربط الوعي مبجال االمن مبتطلبات الوظيفة أو تقييم األداء

- عقد دورات تدريبية بصفة شخصية

- إكمال دورات عرب االنرتنت

- تكون عملية التوعية يف جمال األمن عملية مستمرة!

# السياسات واإلجراءات اخلاصة مبجال أمن األنرتنت

سياسات األمن هي جمموعة من األغراض األمنية للشركة اليت تضمن قواعد السلوك -

للمستخدمني واملديرين وحتدد متطلبات النظام. والقواعد واملتطلبات تكفل بصورة مجاعية أمن الشبكات والبيانات - هذه األغراض

وأنظمة احلاسوب يف املؤسسة.

تساعد املعايري موظفي تكنولوجيا املعلومات للحفاظ على االتساق يف تشغيل -

الشبكات . قائمة من االقرتاحات حول كيفية القيام باألشياء بصورة أكثر فاعلية - اإلرشادات هي

وبأمان.

وتكون وثائق اإلجراءات أطول وأكثر تفصيال من املعاير واإلرشادات. -



## 2018

التحكم يف الوصول عمل للتوعية بشأن أمن املعلومات خريف ورشة



ما هو التحكم يف الوصول

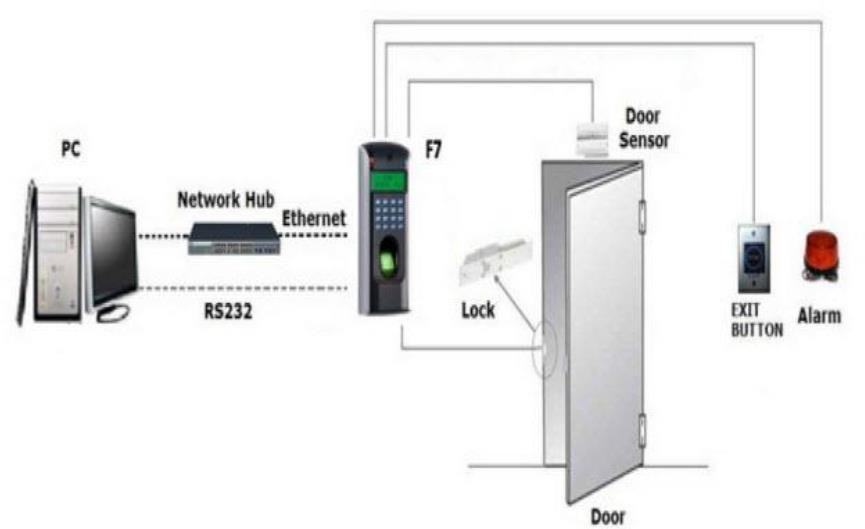
# أمثلة:



***أمثلة على الربامج:***



***التصديق املفاهيم املستخدمني واجملموعات***





- كلمات املرور

- محاية امللف

- قوائم التحكم يف الوصول

# األسئلة

• أي من املستخدمني يستطيع قراءة /كتابة أي من امللفات؟

• هل ملفاتي بأمان فعالً؟

• وماذا يعين أن تكون جذري؟

• ما الذي نريد التحكم به؟

# نظرة عن بعد:

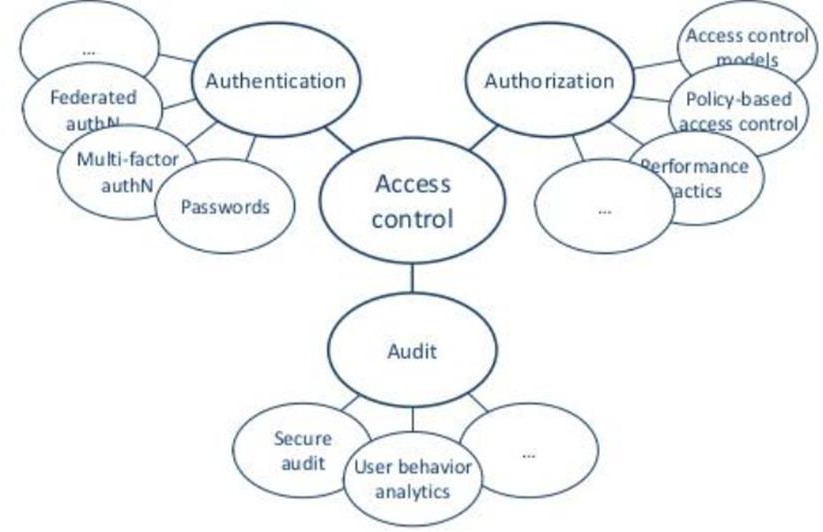


***بعض التفاصيل:***

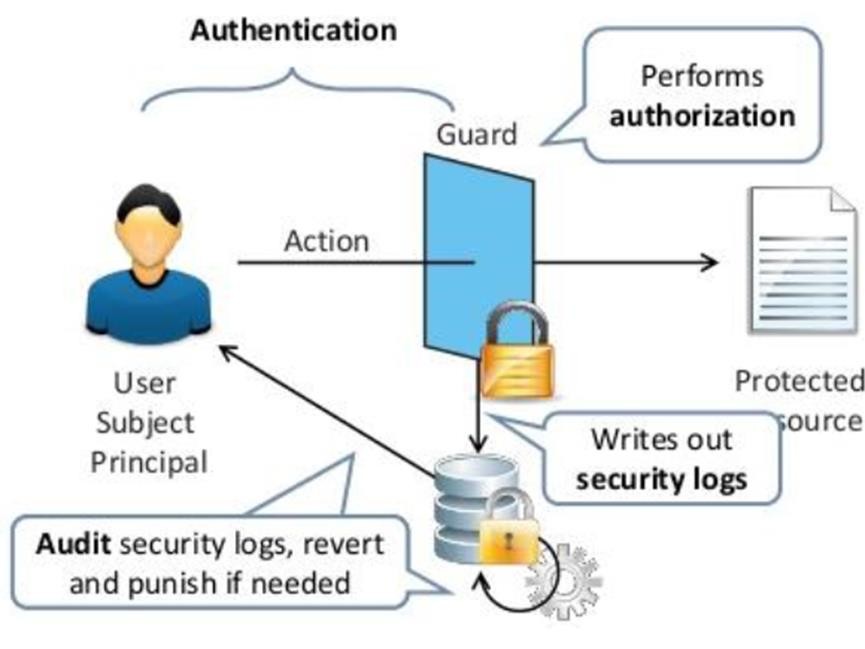


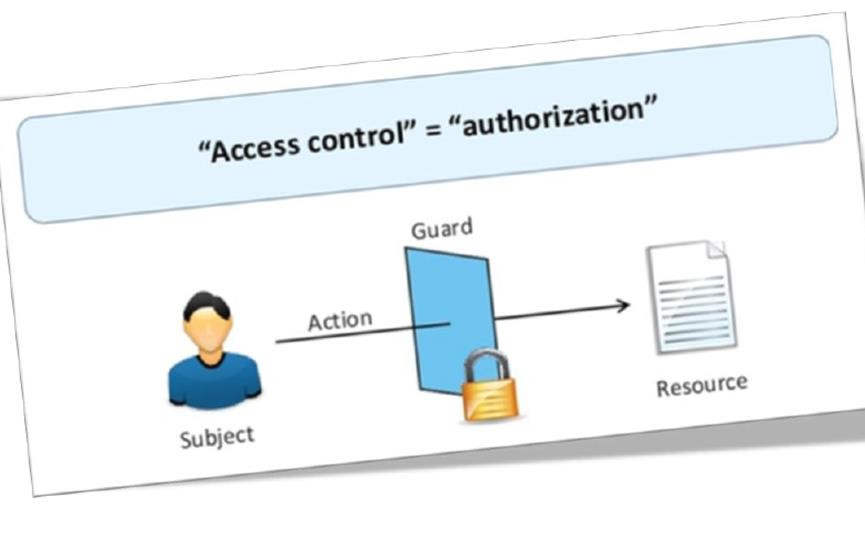


***املزيد من التفاصيل***





***نظرة عن كثب:***

***أخرياً:***



***التصديق***

التصديق فيما ميكن للمستخدم فعلة وما يعجز عن فعلة على الشبكة بعد القيام  يتحكم

بعملية التصديق بنجاح: املستخدم بأثبات هويته، يتفقد النظام موارد الشبكة بعد ما يقوم

اليت ميكن للمستخدم الوصول إليها وما يستطيع املستخدم فعلة بهذه املوارد.

 يستخدم التصديق جمموعة من السمات اليت تصف وصول املستخدم إىل الشبكة.

النظام مبقارنة هذه السمات باملعلومات الذي يتضمنه قاعدة بيانات املصادقة وحيدد  يقوم

جمموعة من القيود هلذا املستخدم وتقوم بتوصيلها إىل املوجه احمللى املتصل به املستخدم.

قواعد املصادقة هي اخلطو األولي يف التحكم يف الوصول. وتضع سياسة املصادقة  وضع

هذه القواعد.

# احملاسبة

احملاسبة عملية رجوعًا إىل شخص أو العملية اليت تقوم بتغري يف النظام وجتمع  تتعقب

املعلومات وتقدم تقارير بشأن استخدام البيانات:

o تستخدم املؤسسة هذه البيانات هلذه األغراض مثل التدقيق أو تقديم الفواتري.

البيانات اجملمعة وقت تسجيل املستخدم سواء كانت عملية التسجيل ناجحة او o تتضمن

باءت بالفشل، كما تتضمن موارد الشبكة اليت توصل إهلا املستخدم.

o يسمح هذا للمؤسسة بتعقب العمليات واألخطاء خالل التدقيق أو التحقيق.

o يتكون تنفيذ احملاسبة من التكنولوجيات والسياسات واإلجراءات والتعليم.

o توفر ملفات السجل معلومات املفصلة بناء على البارامرتات املختارة.



مصفوفة التحكم يف الوصول

• جدول حيدد أذونات.

كل صف يف هذا اجلدول مرتبط بفاعل هو املستخدم أو اجملموعة او النظام o

o الذي ميكن أن يقوم بعمليات.

عمود يف هذا اجلدول مرتبط بكائن وهو امللف أو الدليل أو ال مستند أو اجلهاز o كل

أو املوارد أو أي جهة أخري اليت بشأنها نريد حتديد حقوق الوصول.

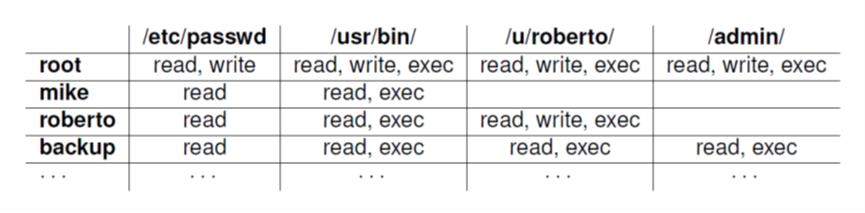
o كل خلية يف هذا اجلدول ممتلئة حبقوق الوصول بشأن اجملموعة ذات الصلة من

الفاعل والكائنات.

o أي خلية فارغة تعين عدم احلصول على حقوق الوصول.

تتضمن حقوق الوصول العمليات مثل القراءة والكتابة والنسخ والتنفيذ واحلذف والتعليق. •

مثال على مصفوفة التحكم يف الوصول:



مشاكل مصفوفة التحكم يف الوصول

قد يكون اجلدول كبرياً للغاية!

:مثال أو rgid أو ruid عملية كل جمموعة1000و مستخدم1000 يضم الذي Unix نظام

egid*أو* *=*10004 *تريليون من اجملاالت*.



النظام 1000ملف/جملدات أو مليون مفعول كائنات (باإلضافة إىل املستخدمني ميتلك نفس

واجملموعات األخرى.)

رابطة مكائن احلوسبة لديها مليون وتريليون خلية!

احلل: قوائم التحكم يف الوصول

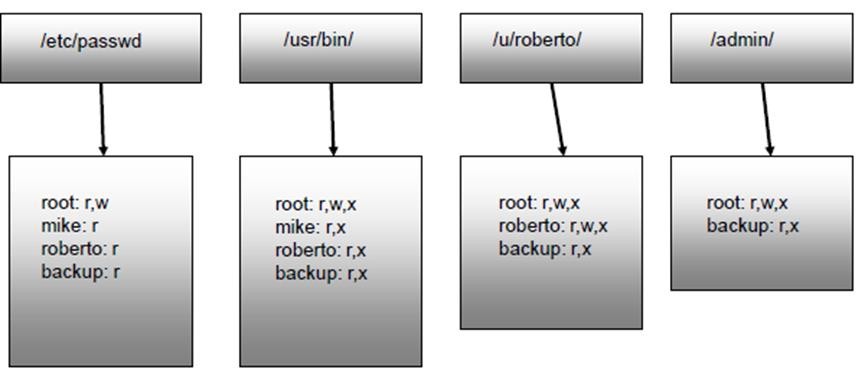
مسؤولية وضع معايري الشبكات على العديد من املنظمات العاملية املختصة بوضع املعايري. تقع

*من األمثلة على هذه املنظمات : منظمة* ISO , IETF , IEEE

# قائمة التحكم يف الوصول

 حتدد لكل كائن، o، قائمة، L، تدعى قائمة التحكم اخلاصة ب o واليت تسرد

املستخدمني الذين لديهم حقوق الوصول بشأن o ولكل مستخدم، s، يعطي حقوق مجيع

الوصول اليت متنحها للمستخدم.

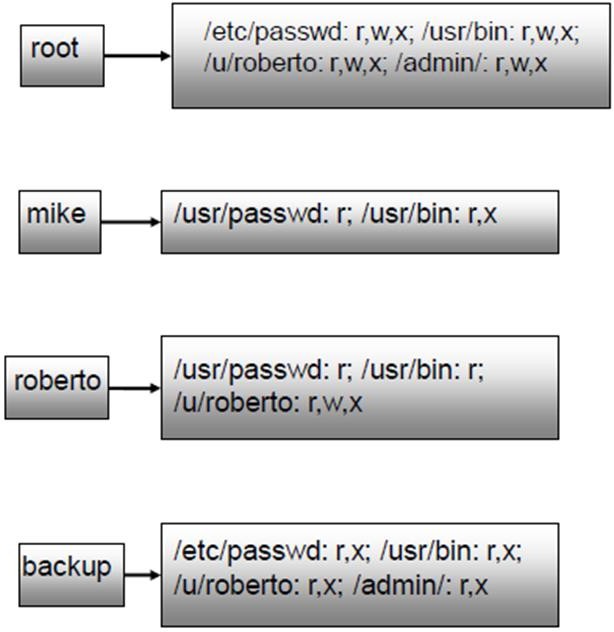
# االمكانيات:

 أخذ منهج املستخدم املستقل للتحكم يف الوصول

مستخدم s قائمة الكائنات اليت ال حتمل التحكم يف حقوق الدخول الفارغة  حيدد لكل

جبانب احلقوق احملددة لكل كائن.



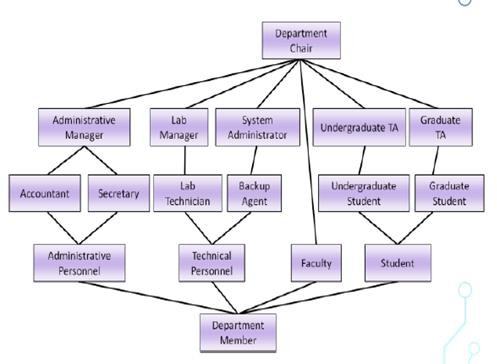


يف الوصول مستند على الدور بعد ذلك حتديد حقوق التحكم يف الوصول التحكم حتديد األدوار ثم

بشأن هذه األدوار فضالً عن تكون مباشرة لألشخاص.

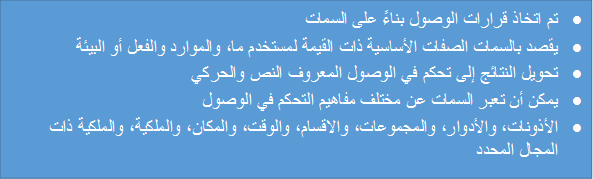
من هذه األدوار يستطيع املستخدم ربط العملية. الدخول عن طريق األدوار-التعامل حتديد أي مستوي املراوغة -إدارة

مع مجيع املستخدمني بهذه الدور والتعبري عن سبب الدخول (أو عدم الدخول(

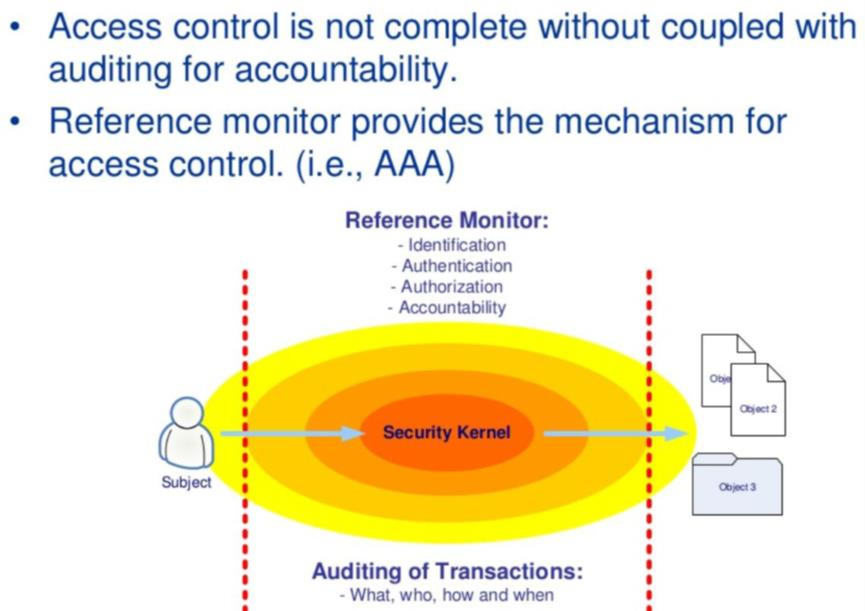




# التحكم يف الوصول بناء على السمات:



***املصادقة التفويض املسؤولية:***



ISO/IEC2700d 

ورشة عمل للتوعية بشأن أمن املعلومات

الوصف

27000 *فئة* 

 معيار إدارة أمن املعلومات آيزو/ آي إي سي

 27000 *املرادف والتعريف*

 27001 *مواصفات* (BS7799-2) *الصادرة يف أكتوبر* 2005

*قانون ممارسة*(ISO17799:2005)

إرشادات تنفيذية

27002 

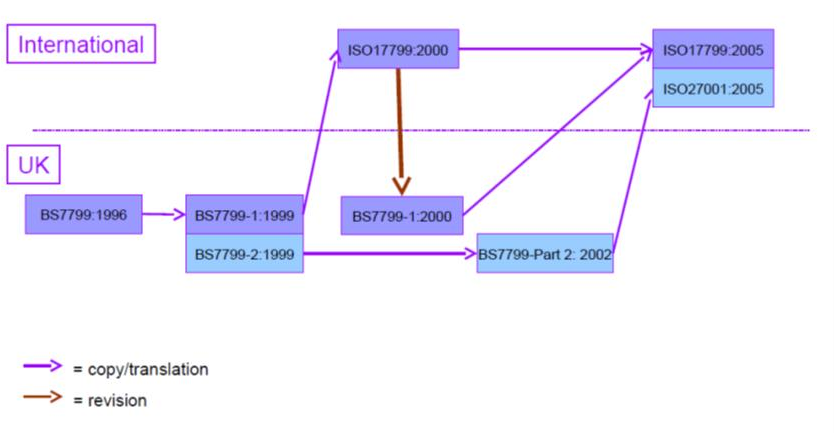
27003 

 27004 *املقاييس والقياسات*

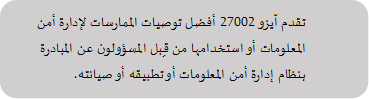
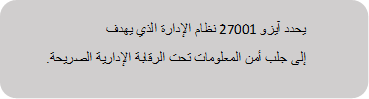


 27005 *إدارة املخاطر* 7799-3*(* *)*BS

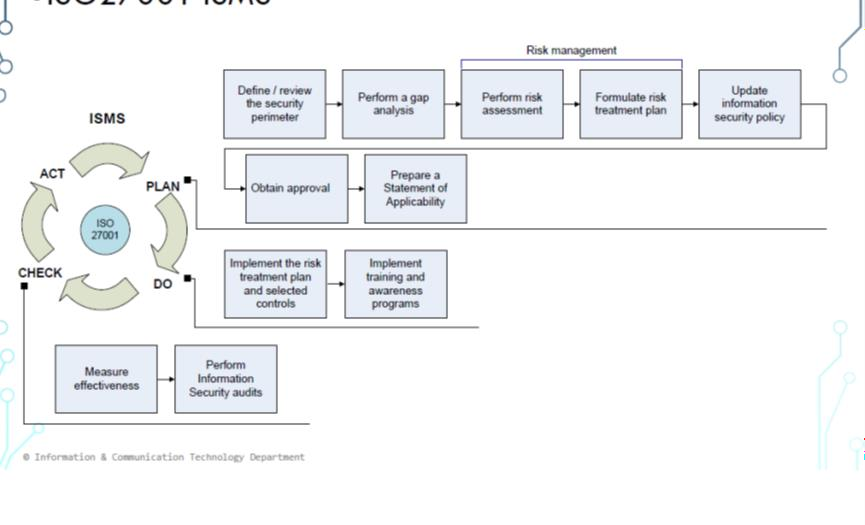
 *تاريخ آيزو* 27001



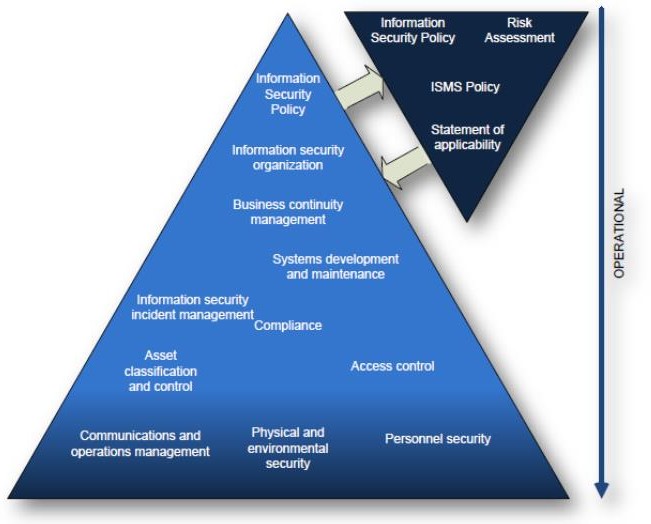
***آيزو* 27000*معايري احلماية***



# آيزو27001 نظام إدارة أمن املعلومات



***آيزو*27002 *اجملاالت:***



االقسام واالهداف



2.1 الربنامج الضار والتعليمة الربجمية الضارة

التميز بني أنواع الربنامج الضار والتعليمة الربجمية الضارة.

2.2 االحتيال

اخلطط والتقنيات واإلجراءات اليت يستخدمها جمرمي االنرتنت. وصف

2.3 اهلجمات

الوسائل املختلفة املستخدمة يف اهلندسة االجتماعية قارن بني أنواع اهلجوم على قارن بني

االنرتنت املختلفة.

2.1 الربنامج الضار والتعليمة الربجمية الضارة:



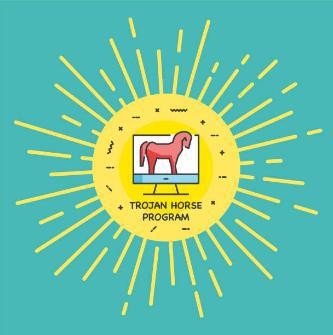
الربنامج الضاره هو مصطلح عام يتألف من مقطعني "ضار" ويعين نية اإلضرار

و"برنامج "

*كلمة الربنامج الضار إلحلاق الضرر بنظام احلاسوب أو احلصول على دخول مصرح" وتعين* "*برنامج مت تصميمه*

# أنواع الربامج الضاره :

***الفريوسات***



***الفريوسات الدودية***

***أحصنة طروادة***



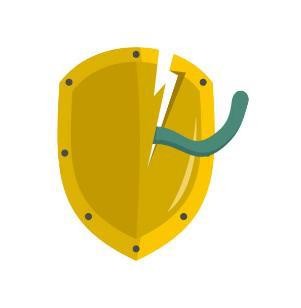
***الفريوسات:***

تعليمة برجمية ضارة قابلة للتنفيذ مرفقة مع ملف تنفيذي أخر. معظم الفريوسات أن تطلق من قبل املستخدم النهائي وتنشط الفريوس هو مثل الربنامج القانوني. حتتاج

يف وقت وتاريخ حمددين.

**الفريوسات الدودية:** هي التعليمة الربجمية الضارة اليت تستنسخ عن طريق االستغالل املستقل املتنقلة عادتاً ما تقلل من سرعة الشبكات. ويف حني الفريوسات املتنقلة ملواطن الضعف يف الشبكات. الفريوسات

الفريوسات إىل برنامج مضيف لتبدأ يف العمل، الفريوسات املنتقلة تستطيع العمل مبفردها. حتتاج

وغري اإلصابة األولية ال حتتاج الفريوسات املنتقلة إىل مشاركة املستخدم.

**أحصنة طروادة:** برنامج ضار حيمل عمليات ضارة على شكل عمليات منشودة مثل اللعب امتيازات املستخدم اليت تقوم بتشغيلها. خيتلف حصان حصان طروادة هو عرب االنرتنت. تستغل التعليمة الربجمية

طروادة عن الفريوس ألنه الطروادة يربط نفسه بامللفات الغري قابلة للتنفيذ.

مثل ملفات الصور وامللفات الصوتية او االلعاب.



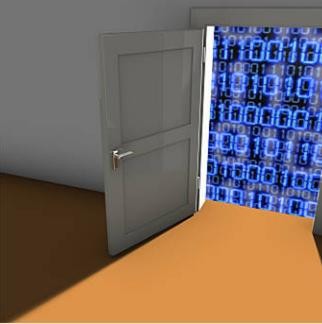
# اخللفية برامج األحتيال األبواب

***برنامج الفدية الضارة***

***الربامج الضارة: القنبلة املنطقية انواع***



***القنابل املنطقية:***



هي برنامج ضار يستخدم مشغل ليقوم بتشغيل التعليمة الربجمية الضارة. على القنبلة املنطقية

املشغالت تواريخ أو أوقات أو برامج اخري تعمل أو حذف حساب املستخدم. حدوث حدث البدء. تقوم القنبلة املنطقية بتنفيذ تعليمة سبيل املثال قد تكون تظل القنبلة املنطقية غري نشطة إىل حني

برجمية ضارة اليت تتسبب يف إحلاق الضرر باحلاسوب.



حني يقوم إىل

***برنامج الفدية الضارة:*** *برنامج الفدية الضارة نظام احلاسوب أو البيانات اليت حيتوي عليها حيتجز*

البيانات يف احلاسوب تشفري



بالدفع. يعمل برنامج الفدية الضارة عادتاً عن طريق املستهدف

باستخدام مفتاح غري معرف للمستخدم.





برنامج الفدية الضارة:

***اخللفية وبرامج االحتيال:*** *االحتيال إىل الربنامج او التعليمة الربجمية اليت ادخلها اجملرم* ***األبواب*** *تشري االبواب اخللفية وبرامج*

أخرتق النظام. تتجاوز األبواب اخللفية املصادقة االعتيادية املستخدمة لدخول النظام. الذي



االحتيال بتعديل نظام التشغيل خللق باب خلفي. بعد ذلك يستخدم املهامجون الباب تقوم برامج

اخللفي لدخول احلاسوب عن بعد.

**الربيد اإللكرتوني واملتصفح:** خدمة عاملية يستخدمها املليارات من األشخاص عرب العامل. واحدة **هجمات** اإللكرتوني ميثل موطن الضعف األساسي الربيد اإللكرتوني هو من أكثر اخلدمات شعبية أصبح الربيد

للمستخدمني واملنظمات.

**برامج التجسس:** هي برامج متكن اجملرم من احلصول على معلومات حول أنشطة الكمبيوتر تتضمن برامج التجسس برامج تعقب النشاطات ، وضغط املفاتيح برامج التجسس األمنية ، تقوم برامج التجسس بتعديل إعدادات اخلاصة باملستخدم. غالبًا ما ومجع البيانات. يف حماولة للتغلب على اإلجراءات

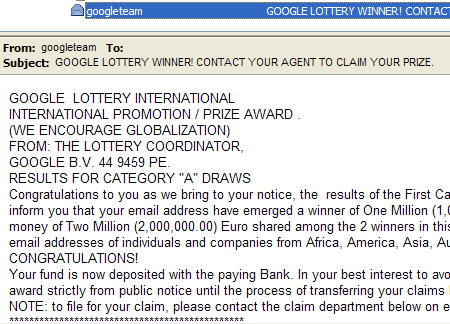
األمان.

**الربيد العشوائي:** املعروف أيضًا باسم الربيد غري املرغوب فيه ، هو بريد إلكرتوني غري مرغوب غري املرغوب فيها طريقة لإلعالن. ومع ذلك، ميكن الربيد املزعج ، فيه. يف معظم احلاالت، تعترب الرسائل

للرسائل غري املرغوب فيها إرسال روابط ضارة أو برامج ضارة أو حمتوى خادع.



مثال عن الربيد العشوائي.



# هجمات الربيد اإللكرتوني واملتصفح.

***برامج إعالنات متسللة:***

برامج اإلعالنات املتسللة العناصر املنبثقة املزعجة خللق طرق ألصحابها. قد حيلل تعرض

الضار اهتمامات املستخدم عن طريق تعقب املواقع اإللكرتونية اليت قام بزيارتها. وبعد الربنامج

ذلك يستطيع إرسال إعالنات منبثقة ذات صلة بتلك املواقع.





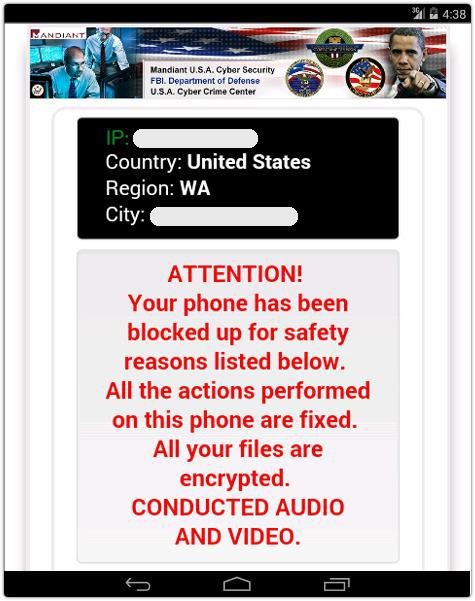
**سكري وير:** املستخدم بالقيام بعملية حمددة نتيجة خلوفهم. يزور سكري وير النوافذ املنبثقة يقنع سكري وير

اليت متاثل نوافذ حوار نظام التشغيل.



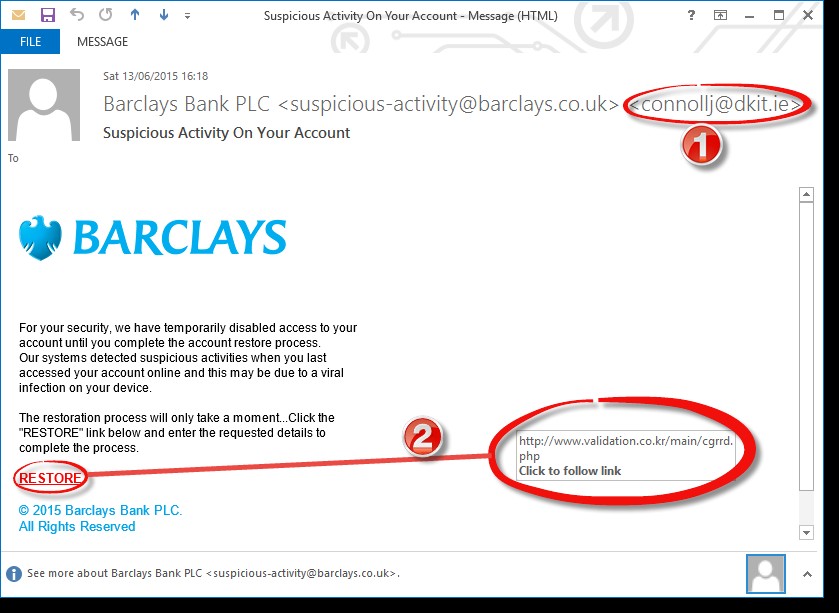






**التصيد األحتيالي:** هو شكل من أشكال االحتيال يستخدم جمرمي األنرتنت الرسائل الفورية مجع معلومات مثل تسجيل الدخول إىل الشبكة أو التصيد االحتيالي حيدث التصيد االحتيالي ووسائل التواصل االجتماعي األخرى حملاولة معلومات احلساب عن طريق طريقة تنكرية كهيئة أو شخص مرموق. بريد إلكرتوني احتيالي متنكر ككونه من مصدر قانوني موثوق عندما يرسل طرف خمادع

هذه الرسالة إىل خداع املستلم إىل تثبيت برنامج ضار على اجلاز اخلاص به. فيه. تهدف



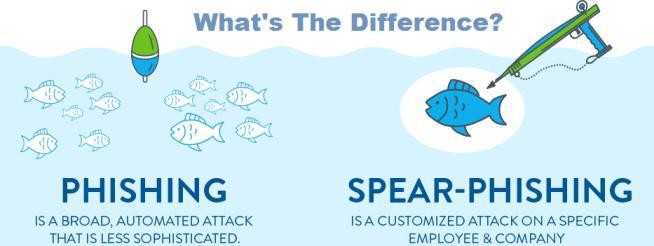


# تغريات التصيد االحتيالي:

احتيالي مو ّجه التصيد االحتيالي املوجة هو هجوم تصيد احتيالي مستهدف. بينما كال تصيد

االحتيالي والتصيد االحتيالي املوجهة يستخدمون الربيد اإللكرتوني للوصول إىل من التصيد

يرسل التصيد االحتيالي املوجهة رسائل الربيد اإللكرتوني املخصص إىل شخص حمدد. الضحايا



عرب األنظمة التليفونية التصيد االحتيالي عرب األنظمة التليفونية هو التصيد االتصاالت. يقوم اجملرمون مبكاملات احتيال عن التصيد االحتيالي اإلنرتنت. كما قد االحتيالي باستخدام الصوت.تكنولوجيا مصادر قانونية باستخدام تكنولوجيا نقل الصوت عرب بروتوكول طريق

يستلم الضحايا رسالة مسجلة قد تبدو وكأنها **قانونية**.





عرب الرسائل النصية القصرية االحتيال عرب الرسائل النصية القصرية هو هجمات االحتيال

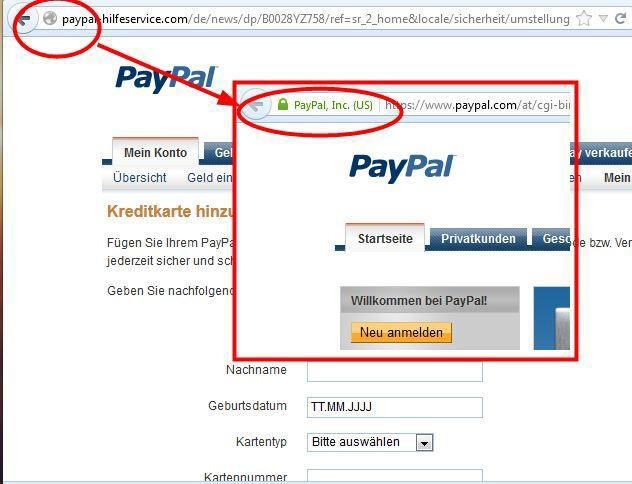
أمنية حيث لكي يقوم بتحميل حصان طروادة أو فريوس أو برامج ضارة أخري إىل أخر. االحتيال عرب الرسائل النصية القصرية هو اختصار ينخدع املستخدم هاتفة احملمول أو جهاز حممول

لكلمة التصيد االحتيالي عرب الرسائل النصية القصرية.



الفارمينج هي تقمس املوقع اإللكرتوني القانوني يف حماولة خلداع املستخدمني إىل فارمينج

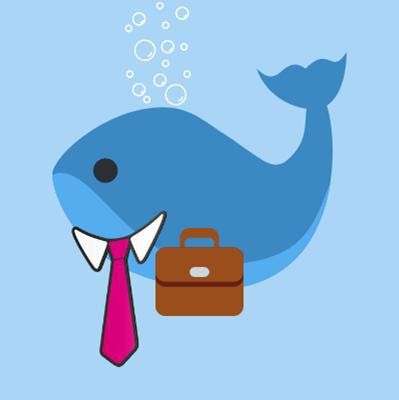
إدخال بيانات اعتماد اخلاصة بهم.





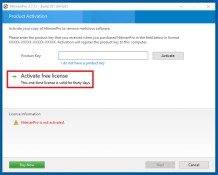
احليتان صيد احليتان هو نوع من أنواع هجوم التصيد االحتيالي الذي يستهدف صيد

اهداف رفيعة املستوي يف املؤسسة مثل كبار املعاونني التنفيذيني.



**خمتطفي املتصفح:** هو برنامج ضار يعدل إعدادات متصفح احلاسوب إلعادة توجيه املستخدم خمتطف املتصفح

اإللكرتونية اتدفع عن طريق عمالء جمرمي األنرتنت. يقوم خمتطفي املتصفح عادتاً إىل مواقع

*بعملية التثبيت بدون إذن املستخدم* ***وعادة ما تكون جزء من درايف باي داونلود.***

**هجمات تسمم نتائج البحث:** البحث مثل جوجل من خالل ترتيب الصفحات حسب ترتيبها وتقديم نتائج البحث اخلاصة باملستخدم. قد تظهر بصورة أكثر أو تعمل حمركات البحث ذات الصلة حسب استعالمات

البحث وذلك وفقاً لصلة حمتوي املوقع اإللكرتوني. حتسني حمرك البحث من أجل حتسني ترتيب املواقع اإللكرتونية عن طريق أقل يف قائمة نتائج هو جمموعة من التقنيات تستخدم

حمرك البحث.

الشركات املتخصصة يف حتسني املواقع اإللكرتونية لتحسني وضعها، حتسني حمرك البحث جلعل املواقع اإللكرتونية الضارة بينما العديد من يستخدم هجمات تسمم نتائج البحث

تظهر بصورة أكثر يف نتائج البحث.

# 2.2 اخلداع:

***مثان دقائق من البحث:***

تصفح االنرتنت وأجد قصة مسلية حول كيفن ميتنيك.



# فن اخلداع:

اهلندسة االجتماعية هي طريقه غري تقينه متاماً حيث يقوم اجملرمني جبمع املعلومات حول اهلدف.

الكشف عن أو

اهلندسة االجتماعية هو هجوم حياول استغالل األفراد إىل اختاذ إجراءات

معلومات سرية.

# تظاهر اخلداع:

يتصل املهاجم بشخص ما ويكذب عليه كمحاولة للوصول إىل البيانات املتميزة. وذلك عندما



ذلك، مهاجم يتظاهر حباجته لبيانات شخصية أو مالية من أجل تأكيد هوية املستلم. مثال على

# شيء مقابل شيء:

عندما يطلب املهاجم معلومات شخصية من طرف مقابل شيء ما، كهدية مثال. ذلك



# أنواع اخلداع:

تطبيقات شولدر سريفينج ودامبسرت دايفينج

انتحال اهلوية واخلدع

بيجي باكينج تيل جاتينج



عرب االنرتنت والربيد اإللكرتوني واخلداع على شبكة



# 2.3 اهلجمات

***اهلجمات األلكرتونية:*** *اخلدمات كنوع من هجوم الشبكات. يؤدي هجوم احلرمان من* ***أنواع*** *هجمات احلرمان من*

ما إىل انقطاع خدمات الشبكات ألجهزة املستخدمني أو تطبيقاتهم. تُعترب كبرية حيث متكنهم من قطع االتصال بسهولة كما الشبكات يف نوع نسبيا إلجراء حتى عن طريق هجمات احلرمان من اخلدمات خماطرة تسبب خسارة فادحة يف الوقت واملال. تُعترب هذه اخلدمات بسيطة

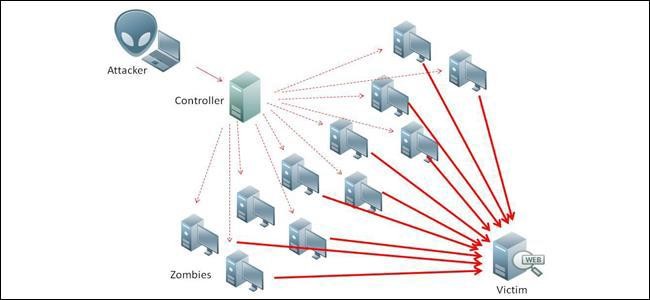
مهاجم غري ماهر.



# 



***هجمات احلرمان من اخلدمات املوزعة***



عملية التجسس مشابهة متاما لعملية التنصت على شخص ما حيدث عندما حيث متر من خالل بطاقة الشبكة اخلاصة بهم بغض **التجسس** - ُتعترب اجملرمني الذين يقومون بتجسس يقوم املهاجم بفحص مرور الشبكة النظر عما إذا كانت تلك عملية املرور موجهة إليهم أم ال.

الشبكات عن طريق تطبيق الربجميات واألجهزة أو مزيج من االثنني.



الربيد االلكرتوني انتحال الربيد اإللكرتوني هو االنتحال اهلجوم، ويستفيد من يف حال يقبل النظامني املصادقة املنجزة من قِبل هجوم انتحال العالقات القامة على الثقة بني نظامني.

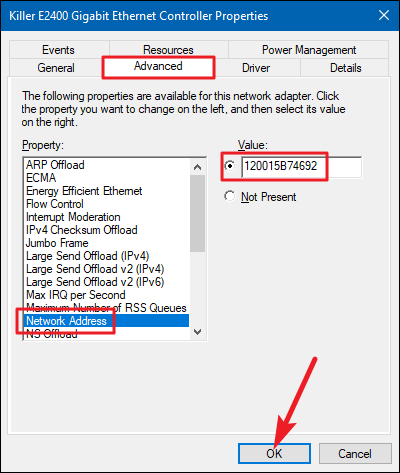
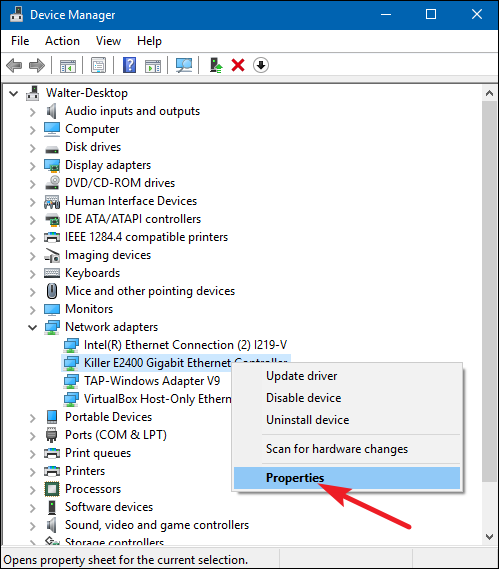


قد ال مير الفرد الذي دخل إىل نظام واحد بعملية التصديق مرة أخرى للدخول بعضهما البعض

إىل نظام آخر.



# عنوان ماك ألنتحال نوافذ ويندوز

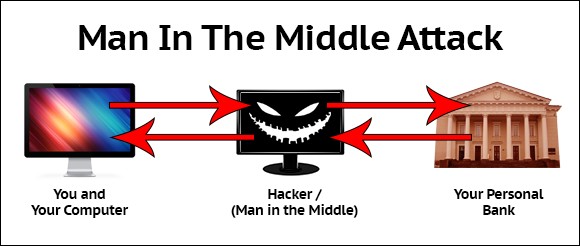


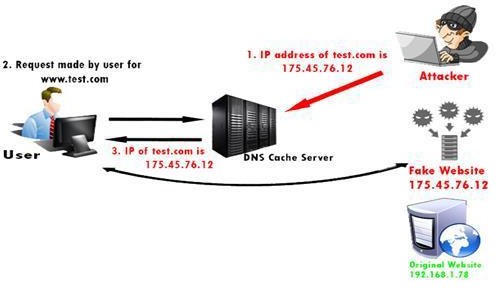
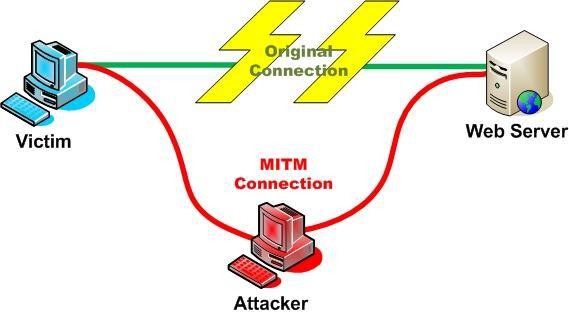
يقوم اجملرم باهلجوم الوسيط عن طريق منع االتصال بني أجهزة ميكن للمجرم أن يقوم بالتالعب بالرسائل ونقل هجوم الوسيط - حبدوث تعديل للرسائل الكمبيوتر لسرقة املعلومات عرب الشبكات. معلومات خاطئة بني املضيفني وذلك ألن املضيفني ليسوا على دراية

يسمح اهلجوم الوسيط للمجرم بالتحكم يف اجلهاز بدون علم املستخدم.











-يشري اهلجوم دون انتظار إىل تهديد دون انتظار وهو هجوم باستخدام الربجميات غري املعروفة أو غري املفصح عنها من قِبل هجوم دون انتظار احلاسوب يف حماولة الستغالل ثغرات

يصف مصطلح ساعة الصفر اللحظة اليت يكتشف فيها شخص ما استغالله. مورد الربجميات.

لوحة املفاتيح -راصد لوحة املفاتيح هو برنامج يقوم بتسجيل أو تدوين الضغط على راصد

مستخدم الربنامج. ميكن للمجرمني تنفيذ برامج ضغط املفاتيح من خالل أو من خالل االجهزة املتصلة فعليا جبهاز الكمبيوتر. يقوم املفاتيح من قِبل املفاتيح إلرسال ملف السجل بالربيد برامج مثبتة على نظام الكمبيوتر اجملرم بتشكيل برنامج مسجل ضغطات لوحة

تقوم ضغطات املفاتيح اليت مت تسجيلها يف ملف السجل بكشف أمساء اإللكرتونية اليت مت الدخول عليها واملعلومات احلساسة اإللكرتوني قد املستخدمني وكلمات املرور واملواقع

 األخرى.

# 

*هجمات التطبيقات:* ***الربجمة عرب املواقع***

املواقع هي نقطة ضعف موجودة يف تطبيق الويب تسمح الربجمة عرب املواقع حقن الربجمة عرب

عليها من قِبل

العميل تشمل على برجمية ضارة يف صفحات الويب املطلع من جانب

نصوص

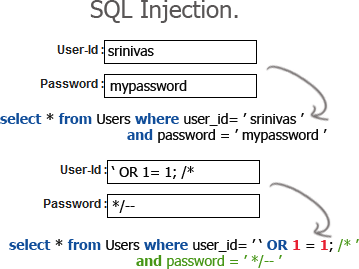
حتتوي عملية الربجمة عرب املواقع على ثالثة مشاركني وهم: اجملرم والضحية واملوقع اإللكرتوني الضحية بصورة مباشرة ولكن يستغل نقطة الضحية. اإللكرتوني. ال يستهدف اجملرم

الضعف داخل املوقع اإللكرتوني أو تطبيق الويب.



**هجمات الربجمة باحلقن** قاعدة بيانات مثل قاعدة بيانات إس كيو إل (لغة االستعالمات البنيوية) أو لالمتداد من أجل ختزين البيانات باملوقع اإللكرتوني بطريقة ميكن استخدام يف الربنامج مثل عدم التحقق من صحة قاعدة بيانات لغة الرتميز القابلة تقليدية. تستغل هجمات الربجمة باحلقن نقاط الضعف

استعالمات قاعدة البيانات بصورة صحيحة.

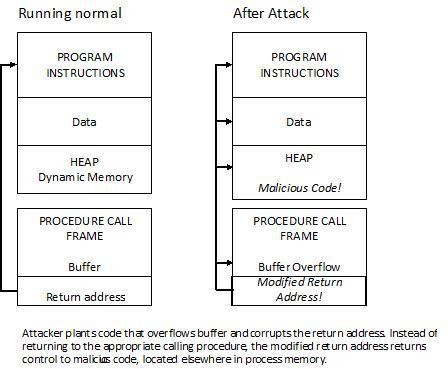


# جتاوز سعة املخزن

املخزون املؤقت عندما تتجاوز البيانات حدود املخزون املؤقت. املخازن املؤقتة بتغيري البيانات خارج حدود املخزن املؤقت، يقوم حيدث جتاوز سعة هي مناطق ذاكرة خمصصة للتطبيقات.

إىل الذاكرة املخصصة لعمليات أخرى. ميكن أو يؤدي إىل تعطل النظام أو التطبيق بالوصول

# اخرتاق البيانات أو تقديم تصاعد االمتيازات.



***التحكم آكتيف إكس وجافا*** *آكتيف إكس جزء من الربجميات املثبتة من قِبل املستخدم لتوفري* ***ضوابط*** *ُتعترب ضوابط التحكم*

قدرات ممتدة.



حتكم آكتيف إكس غري املوثوق فيها/ جمهولة ضوابط حتكم ضارة. أو تثبيت برامج ضارة أو تسجيل ضغطات املفاتيح. كما قد تكون ضوابط ميكن هلا مراقبة عادات التصفح

حتكم آكتيف إكس يف تطبيقات مايكروسوفت األخرى. من خالل شارح، آلة جافا االفرتاضية. تتيح آلة جافا االفرتاضية تعمل ضوابط الربجمة غري املوثوق فيها من بقية نظام وتعمل ضوابط حتكم جافا وظيفة برنامج جافا. تقوم آلة جافا االفرتاضية بعزل

هناك نقاط ضعف تسمح للربجمة غري املسموح بها بنشر القيود املفروضة. التشغيل.

***التحكم آكتيف إكس وجافا*** *تنفيذ املدونة الربجمية عن بعد جملرم االنرتنت يف تنفيذ الربجمية* ***ضوابط*** *تسمح نقاط ضعف عمليات*

إىل التحكم يف النظام بامتيازات املستخدم الذي يقوم بتشغيل التطبيق. عن بعد للمجرم تنفيذ أي أمر على اجلهاز املستهدف الضارة باإلضافة يسمح تنفيذ املدونة الربجمية

# مكافحة هجمات التطبيق

• قم بكتابة تعليمة برجمية صعبة

النظر عن اللغة املستخدمة أو مصدر املدخالت اخلارجية، قم بتطبيق برجمة • بصرف

سديدة للتعامل مع كافة املدخالت اخلارجية باعتبارها عدائية .

• حتقق من صحة كافة املدخالت كما لو أنها عدائية.

بكافة الربجميات مبا يف ذلك أنظمة التشغيل والتطبيقات احملدثة وعدم جتاهل • احتفظ

حتديث املطالبات.

• ال يتم حتديث الربامج تلقائيا لذا على األقل دائما .

قم بتحديد اختيار حتديث الدليل.

# امللخص

ونقاط الضعف واهلجمات حماور أساسية للمتخصصني يف األمن اإللكرتوني . ُتعترب املخاطر

هذه الدورة خمتلف هجمات األمن اإللكرتوني اليت يقوم بها جمرمي اإلنرتنت. • تغطي

• تشرح هذه الدورة خماطر الربامج والتعليمة الربجمية الضارة.

تغطي اجللسة أنواع اخلداع املتعلقة باهلندسة االجتماعية. تشرح املناورة كافة أنواع •

اهلجمات اليت جتربها الشبكات السلكية والالسلكية.

النهاية، جيري نقاش حول نقاط ضعف املقدمة يف هجمات التطبيقات خالل الدورة. • ويف



كافة أنواع املخاطر احملتملة فإن ذلك يسمح للمؤسسة حتديد نقاط الضعف أن تتعلم كيفية محاية نفسها من خداع األمن ومن خالل فهم اليت قد جتعلها مستهدفة. ميكن للمؤسسة

اإللكرتوني واملناورات.

**دورة عملية:**



*احلماية* ***تأمني الشبكة***

# محاية تأمني الشبكات أثناء تصميم الشبكة

 جدر احلماية

 تصفية احلزمة

 فحص احلزمة املناسبة

# 



***خوادم وكيل فحص احلزمة الشامل***

 منطقة منزوعة السالح

 أنظمة الكشف عن حماوالت التدخل

# الكشف عن الدخالء بالشبكة

 يعتمد على التوقيع

 يعتمد على العيوب

**-** مواجهة البيانات

**-** شبكة خاصة أفرتاضية املُبينة

# أساسيات كلمة املرور

 أساسيات كلمة املرور ومبادىء فهم احلاجة اىل كلمة املرور

 طول كلمة املرور

 تعقيد كلمة املرور

 إنشاء كلمة املرور وتقنيات احلفظ

# التكرار

 مواجهة الكوارث

 استمرارية االعمال

o أمثلة املشروعات املتوقفة

# املمارسة

 تعطيل الكود: هجوم عنيف، هجوم املعجم

 برنامج واير شارك

التوعية بشأن أمن املعلومات

# التشفري )سري أو خمبأ(

 التشفري ⎯ فن وعلم "األكواد السرية" وإعدادها واخرتاقها

 التشفري ⎯ إعداد "األكواد السرية"

o التشفري- فك التشفري

 حتليل الشفرات ⎯ اخرتاق "األكواد السرية"

 التشفري ⎯ كل ما سبق (وأكثر)

# كيف ميكنك التشفري

● تستخدم الشفرة أو نظام التشفري لرتميز الرسالة غري املشفرة

● وتكون نتيجة التشفري نص مشفر

● نقوم بفك التشفري النص املشفر السرتداد الرسالة غري املشفرة

● يستخدم املفتاح لتكوين نظام التشفري

● يستخدم املفتاح املتماثل بنظام التشفري نفسه سواء عند التشفري أو فك التشفري

● يستخدم املفتاح العام بنظام التشفري نفسه سواء عند التشفري أو فك التشفري

# أفرتاضات أساسية

● أن النظام معروف بالكامل للمتطفل

● ويكنون املفتاح وحده سر

● وال تكن خوارزميات التشفري سر

وتعرف بأسم مبادىء كري شوف

ماذا نقوم بهذا األفرتاض؟

● أظهرت اخلربة أن اخلوارزميات السرية تصبح ضعيفة عند التعرض هلا

● وال تظل اخلوارزميات سرية

● ومن االفضل إجياد الضعف مُسبقاً

# التشفري مثل الصندوق األسود

األجزاء الغري معروفة

رسالة غري



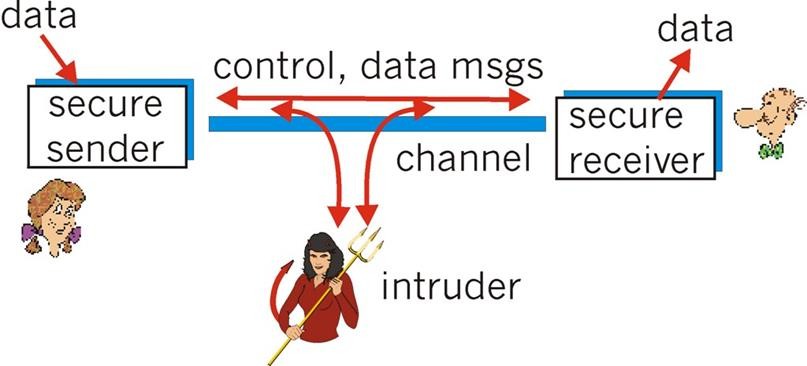
املفتاح

النص املشفر

املفتاح

رساله غري مشفرة

# األصدقاء واألعداء: أليس وبوب وترودي



من قد يكون بوب، وأليس؟

• **…**حسنًا، يف أرض الواقع يكون بوب وأليس!

• متصفح الويب/ اخلادم للتعامالت اإللكرتونية (مثال الشراء عرب اإلنرتنت)

• عميل/اخلادم احلساب املصريف عرب اإلنرتنت

• خوادم نظام أمساء النطاقات

• تتبادل املوجهات حتديثات مسارات التوجيه

*...* •



# تصنيف التشفري

• املفتاح املتسق

o نفي املفتاح للتشفريوفك التشفري

o نوعان: عمليات تشفري التدفق، عمليات تشفري احلظر

• املفتاح العام )أو التشفري غري املتماثل(

o مفتاحان، واحداً للتشفري )عام(، وواحد لفك التشفري )خاص(

o أيضًا، ال يقارن أي شيء ا بالتوقعات الرقمية مع تشفري املفتاح املتسق

• خوارزميات التجزئة

o يف بعض األوقات يُنظر إلية باعتباره " أحد أساليب" التشفري

# تصنيف حتليل التشفري

• من وجهة نظر املعلومات املتوفرة للمتطفل

o النص املشفر فقط جمرد معروف خمتار o نص o نص جمرد

 "هجوم وقت الغداء"

 قد تقوم الربوتوكوالت بتشفري البيانات املختارة

o نص جمرد خمتار بتكييف

o املفتاح املتعلق

o حبث إعادة التوجية

o واالخرين ...

# التشفري املتسق

m=رسالة النص اجملرد،

=c الشفرة (رسالة مُشفرة)

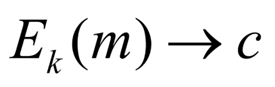


تود أليس التحويل إىل بوب سرًا

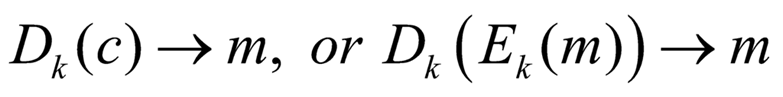
Ek(m)→c

الحظ أن املفتاح هو نفسه بالنسبة لكالً من بوب وأليس

األسئلة: كيف ميكنهم تبادل املفتاح ألول مرة حيث أنهم يودون التحدث سرًا؟

يقوم بوب بتشفري )E( والرسالة با )m( مع املفتاح )k(

تقوم أليس بفك تشفري )D( وشفرة )c( للحصول على رسالة )m(

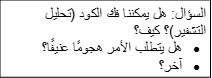


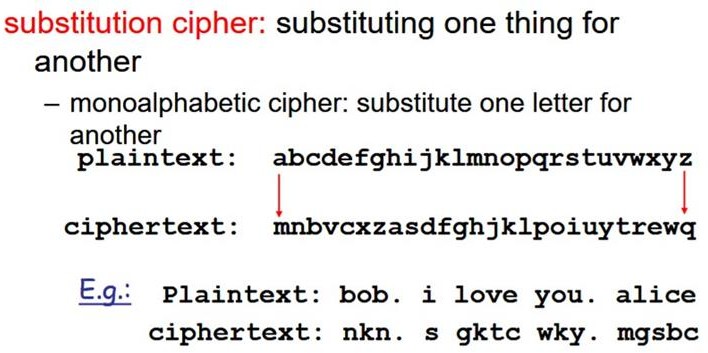
***تصنيف املفتاح املتسق*** *االستبدال: استبدال شيء بآخر فرة*

شفرة األجبدية املوحدة: استبدال حرف باآلخر حروف

: abcdefghijklmnopqrstuvwxyz *اهلجاء*

املفتاح: 3

*الرسالة: بوب إنين أحبك النص املشفر:* brx oryh l ere



# تشفري املفتاح اخلاص

التشفري املتماثل -تستخدم اخلوارزميات املتماثلة- لتشفري البيانات وفك تشفريها، كما يُعرف األسلوب بتشفري املفتاح عملية املتسق. تستخدم بعضًا من مقاييس التشفري مفتاح املشاركة املُسبقة اخلاص. تستخدم أنظمة التشفري املتعددة التشفري

املشرتكة التشفري املتسق الذي يتضمن اآلتي:

 مقاييس

 خوارزم

 مقاييس تشفري البيانات

# تصنيف املفتاح العام

لسؤال: كيف املوافقة على املفتاح يف املقام األول (حتدي ًدا إن مل يسبق هلم "االلتقاء)"

يف تصنيف املفتاح املتسق يشارك كالً من الراسل واملستقبل نفس املفتاح السري.

هي احلاجة لعمل توزيع مؤمن (تأسيس) برأس املفتاح السري:

بتصنيف

واملشكلة األساسية

املفاتيح السرية لعمليات اإلرسال قبل إرسال الرسالة نفسها.

 قدم ديفي وهيلمان منوذج جديد

 تناظر صندوق الربيد:

o قام بوب بتأمني صندوق الربيد

ولكنها مل تستطع إلغاء التأمني الستخراج بالصندوق،

o تستطيع أليس إدخال حرف

رسالة الربيد

o ميتلك بوب املفتاح وبإمكانه استخراج الرسالة

 رسائل مشفرة لبوب مع مفتاحه العام

o يستطيع التوزيع حبرية

 يقوم بوب بفك تشفري رسائله باستخدام مفتاحه اخلاص

o بوب الوحيد الذي يعلم هذا

كيف يعمل خمطط املفاتيح العامة؟ الشروط الثالثة األساسية:

يكون من السهل تشفري الرسالة ذات املفتاح املالئم أو فك تشفريها بطريقة حسابية  جيب أن

تكون غري قابلة للتطبيق من الناحية احلسابية وذلك الستخالص مفتاح خاص من  جيبأن

املفتاح العام

تكون غري قابلة للتطبيق من الناحية احلسابية لتحديد املفتاح اخلاص من هجوم  جيبأن

النص اجملرد املختار

o يستطيع املتطفل اختيار أي رسالة وتشفريها واحلصول على النص املشفر

**استبدال املفاتيح** التواصل باستخدام شفرة الكتل لتشفري رسائلهم، ولكنهم ال ميتلكون مفتاح يريد أليس وبوب

مشاركة

كيف حيصل كالً من أليس وبوب على مفتاح مشاركة؟

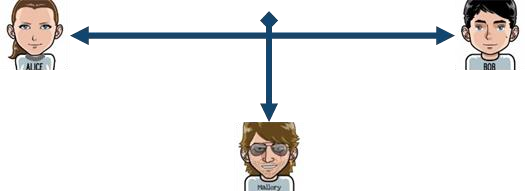


# احلل األول

 تُرسل أليس املفتاح باإلضافة إىل رسالتها املشفرة

 تطلع مالوري على الرسالة املشفرة واملفتاح

 يستخدم املفتاح لفك تشفري الرسالة



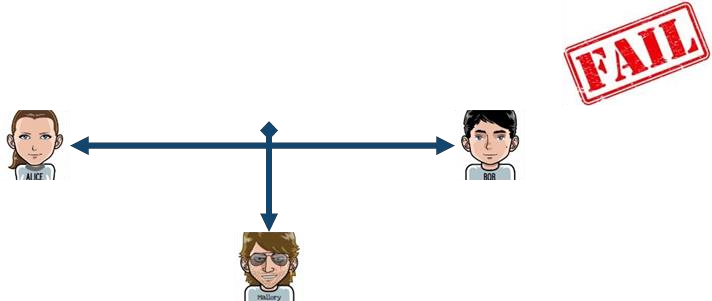
# احلل الثاني

 يُرسل أليس مفتاح يف وقت ما قبل إرسال بوب للرسالة املُشفرة

 يضطر مالوري أن ينتظر لوقت أطول إذا رأى حتويل املفتاح، واآلن هو ميتلك

 املفتاح

 يستخدم املفتاح لفك تشفري الرسالة



**الثالث -استخدام تشفري املفتاح العام** يستخدم املفتحان: أحدهم للتشفري الذي خيتلف عن املفتاح املستخدم **احلل** مفتاح فك التشفري املستند إىل معلومات مفتاح عملية تشفري املفتاح العام لفك التشفري. ال يستطيع اجملرم حساب

التشفري، والعكس، بأي فرتة زمنية معقولة. تتضمن اخلوارزميات غري املتماثل:

تعمية باملنحنيات اإلهليجية -يستخدم املنحنيات اإلهليجية كجزء من اخلوارزميات. 1 .

الواليات املتحدة األمريكية، تستخدم وكالة األمن القومي األمريكية تعمية ففي

باملنحنيات اإلهليجية جليل التوقيع الرقمي واستبدال املفتاح.

تشفري اجلمل -تستخدم مقاييس احلكومة األمريكية للتوقيعات الرقمية. ومتتلك هذه 2 .

اخلوارزميات حرية االستخدام ألن ال أحد حيمل االمتياز.

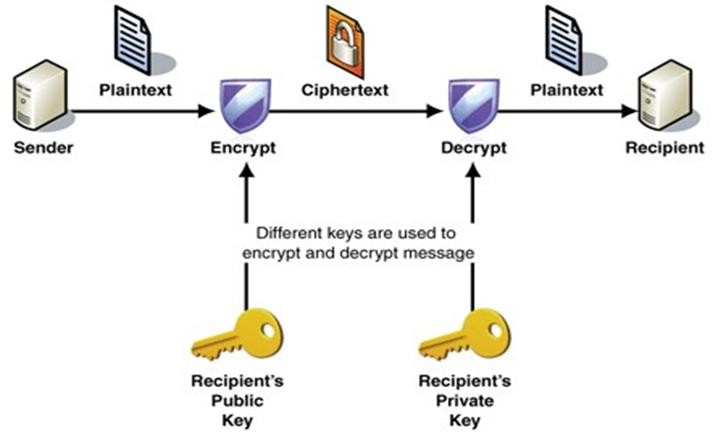
تبادل مفتاح ديفي-هيلمان -يوفر أسلوب تبادل إلكرتوني ملشاركة املفتاح السري. 3 .

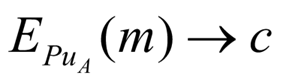
مفتاح ديفي-هيلمان الربوتوكوالت املؤمنة مثل بروتوكول طبقة املنافذ اآلمنة، وبروتوكول النقل اآلمن، وحزمة بروتوكول تستخدم تبادل اآلمنة، وبروتوكول طبقة املقابس

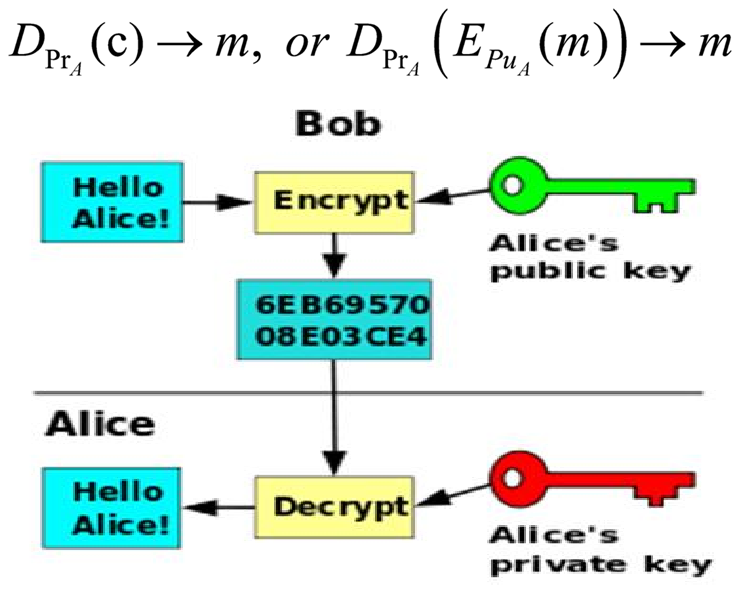
اإلنرتنت األمنية.

خوارزمية آر إس إيه -يستخدم منتج من رقمني أساسيني كبريين ذات طول متساوي 4 .

100 و200 رقم. تستخدم املتصفحات خوارزمية آر إس إيه لتأسيس االتصال املؤمن. بني



يقوم بوب بتشفري (E) والرسالة با (m) مع مفتاح أليس العام

تقوم أليس بفك تشفري )D( وشفرة )c( للحصول على رسالة )m(

 تبادل مفتاح ديفي-هيلمان



g ≠ 0, g ≠ 1, and g ≠ p-1 o

 ختتار أليس مفتاحها اخلاص kA

o *يقوم حساب* gkA = KA *بتعديل* p *ويُرسلها إىل بوب بالتحديد*

 خيتار بوب مفتاحه اخلاص kB

o حسابB=9KB تعادلP وإرساهلا إىل أليس يف الوضع السليم

أراد أن يتفق أليس وبوب على برهان مشرتك، قاموا حبساب أ سر مسرتك س  عندما

SA.B=KB k p*تعادل* 

SBA=KA KB p*تعادل* 

ملاذا يتم استخدام املعادالت اخلاصة بديفي؟

sA,B=SA,B 

(gkA)kB mod p = (gkB)KA mod p 

يعرف مالوري:

G and p 

Ka and KB 

ملاذا ال حياسب مالوري السر؟



كان هذا أول برهان ملخطط التشفري

# املعادالت الصعبة

تقوم عمليات التشفري الرئيسية العامة على املشاكل الصعبة

تقوم معدالت ديفي-هيلمان على مشاكل لوغاريتمات املنفصلة املقدمة :

• جمموعة املضاعفةG

a in G*عنصر* •

• اجياد الناتجb

• *احلل الفريد ل*G in b = ax

b*لوغل*x •

ال توجد خوارزمية متعددة احلدود حلل هذه املسالة\*

البيانات وحجمها

الصغرية

***املتماثلة لفك التشفري األساسي العام*** *يعترب التشفري هو أكثر كفاءة يف محاية سرية* ***املقارنة*** *األداة األساسية*

جيعلها أكثر أمانًا ملهام مثل تبادل األدوات اإللكرتونية وهي كمية صغرية من وسرعتها



البيانات بدالً من تشفري كتل كبرية من البيانات.

تعترب أنظمة فك التشفري أكثر فعالية وميكن التعامل معها املزيد من البيانات وعلى متماثل

ذلك، اإلدارة األساسية ألنظمة فك التشفري تعترب األكثر تعقيداً ويصعب التعامل معها. الرغم من

# استخدامات التشفري الرئيسي العام

 السرية

o نقل البيانات عرب قناة غري آمنة

o ختزين آمن على وسائط إعالم غري أمنه

 املصادقة (يف وقت الحق)

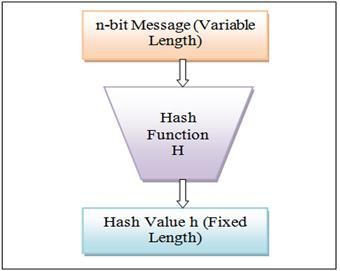
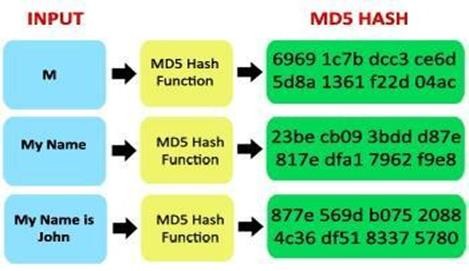
 توفر التوقيعات الرقمية النزاهة وعدم التنصل

o ال يوجد مفاتيح متماثلة لعد التنصل

# داالت جتزئة

أيضاً: األبواب السرية، دالة ذات اجتاه واحد عن طريق أخذ بيانات ثنائية (الرسالة) وتقديم أطوال ثابتة وتسمي التجزئة أداة تضمن نزاهة البيانات

ومتثيل يسمي قيمة جتزئة أو تشفري الرسالة.



**خوارزميات التجزئة** ذات اجتاه واحد اليت من اليسري نسبياً أن يتم حماسبتها ولكن يصعب حبوب القهوة قياس جيد لدالة ذات اجتاه واحد. من تعترب التجزئة دالة هذه القطع الصغرية مرة آخري أو بدرجة كبرية عكسها. يعترب طحن السهل طحن حبوب القهوة، ولكن من املستحيل أن تعيد

تعيدها إىل أصلها .

تتميز دالة التجزئة التشفريية باخلصائص التالية :

 من املمكن أن تكون املدخالت طويلة .

 حتتوي املدخالت على طول ثابت .

 تعترب دالة التجزئة ذات اجتاه واحد وال يكمن عكسها .

 أثنني من قيم املدخالت سوف ينتج قيم جتزئة خمتلفة.

العديد من خوارزميات التجزئة احلديثة تُستخدم على نطاق واسع اليوم. وأشهر أثنني  يوجد

*من هذه اخلوارزميات هي* MD5 *و*SHA.

خوارزمية (MD5) تشفري الرسالة هي خوارزمية جتزئة طورها رون ريفست اليت تنتج قيمة 

*جتزئة* 128 *بايت* .

– (SHA)خوارزمية جتزئة أمنة اليت طورها املعهد األمريكي الوطين للمعايري والتقنية، 

وميكن تنفيذها يف أطوال خمتلفة :

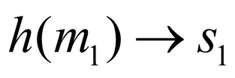
SHA- 224 (*بايت* 224) o

SHA- 256 (*بايت* 256) o

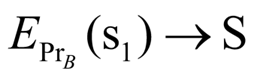
SHA- 384 (*بايت* 384) o

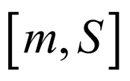
SHA- 512 (*بايت* 512) o

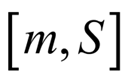
# املصادقة

 يكتب بوب رسالة إليّ وحيسب تشفري الرسالة (أو التوقيع(

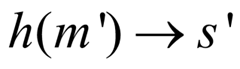
 ُيشفر بوب التوقيع عن طريق املفتاح اخلاص به



 يرسل بوب رسالة (إشعار بإتاحة الرسالة لكل فرد) باإلضافة إىل توقيعه

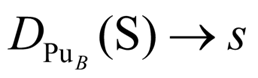
ُمصدقة

ألي فرد أن يستخدم املفتاح الرئيسي لكي خيترب إذا كانت الرسالة ميكن

 جيوز ألي شخص أن يقوم بعملية الفحص، إذا صرح بوب باآلتي:



o احلصول على طريقة تشفري الرسالة

o احلصول على املفتاح الرئيسي اخلاص بوب. تشفري التوقيعS الذي يقدم ملخصاً

إذا كان نعم، فالرسالة تعترب مُصدقة S’ = S فحص

وهذا يعنى أن ما قاله بوب صحيح للغاية واليت يقصد بها (م )1



التوقيعات الرقمية والشهادات

# التوقيعات والقانون

التوقيعات الرقمية نفس اخلصائص الوظيفية مثل التوقيعات التحريرية اخلاصة تقدم

باملستندات اإللكرتونية .

التوقيع الرقمي لتحديد ما إذا قام الشخص بتعديل املستند بعد توقيع املستخدم علية . يُستخدم

الرقمي طريقة رياضية مستخدمة لفحص مصادقة ونزاهة الرسالة واملستندات يعترب التوقيع

الرقمية والربجميات .

من البلدان، فإن العديد من التوقيعات الرقمية لديها نفس األهمية القانونية كما وفى العديد

هو احلال بالنسبة للمستندات املُوقع عليها خبط اليد .

وتوفر التوقيعات الرقمية أيضاً عمليات اإلنكار.





# كيفية عمل تكنولوجيا التوقيع الرقمي

تعترب عملية التشفري غري املتناظرة هي أساس التوقيعات الرقمية .

التوقيعات الرقمية:

العمومي للخوارزميات مثل RAS مفتاحان رئيسان: مفتاح منهما خاص واآلخر عام. ينتج املفتاح

# تعترب املفاتيح متصلة رياضياً.



***أساسيات الشهادات الرقمية*** *الرقمية مبثابة جوازات السفر اإللكرتونية تعترب الشهادة*

الشهادات الرقمية للمستخدمني والضيوف واملنظمات لتغيري املعلومات اخلاصة بهم عرب تضمن

األنرتنت . الرقمية وحتقق بأن املستخدمني الذين يقومون بإرسال رسالة هم األشخاص توثيق الشهادات

الذين يطالبون حبقهم . تقدم الشهادات الرقمية الطابع السري للمستخدم باإلضافة إىل الوسائل من املمكن أيضاً ان

اليت تعمل على تشفري أي رد.

# 



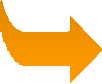
**شهادات رقمية** الرقمية هيكل موحد حتى يستطيع استيعاب وقراءة ذلك بغض النظر **إنشاء** جيب أن تتيع الشهادات

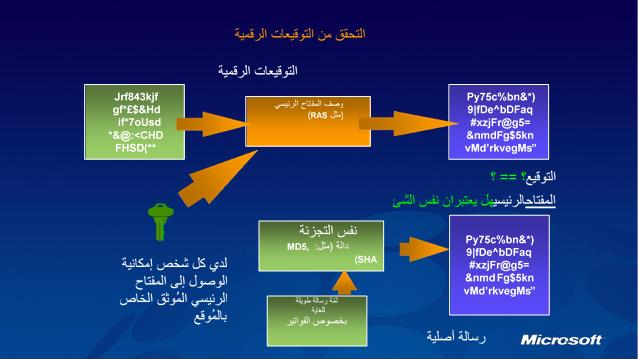
عن اجلهة ا ُملصدرة .

X.509 هو املعيار اليت يستخدم يف انشاء الشهادات الرقمية واملفتاح الرئيسي للبنية يعترب

اخلاصة ب (PKI) املستخدم فى إدارة الشهادات الرقمية . واألحكام واإلجراءات الالزمة لإلنشاء وإدارة وتوزيع واستخدام التحتية تعترب PKI هي السياسات

وختزين وإلغاء الشهادات الرقمية.





# بروتوكول طبقة الوصل اآلمنة/ بروتوكول

**SSL *يقصد به (بروتوكول طبقة الوصل اآلمنة)***



(بروتوكول أمان طبقة النقل )

● خدمة بروتوكول طبقة الوصل اآلمنة

● طورت من خالل شركة نتسكيب

● صُممت النسخة رقم 3 مبدخالت عامة

بعد ذلك معيار االنرتنت ا ُملعروفTLS ● وتصبح

● استخدامات بروتوكول التحكم باإلرسال لتوفر خدمات كاملة ميكن االعتماد عليها



● حتتوي طبقة الوصل اآلمنة على طبقتني من الربوتكوالت

# بروتوكول طبقة الوصل

● ُتعرف شركة نتسكيب بربوتوكول طبقة الوصل اآلمنة (التدفقات) 1994

● نُشرت بروتوكول طبقة الوصل اآلمنة النسخة 2.0 مؤخراً عام 1995



● ُنفذت النسخة 2.0 يف منتجات شركة نتسكيب يف منتصف عام 1995

● تفاوت شركة مايكروسوفت (معاهدة التعاون بشأن الرباءات) عام 1995

● نُشرت بروتوكول طبقة الوصل اآلمنة النسخة 3.0 بنهاية عام 1995

النسخة 2.0 يف منتجات شركة نتسكيب يف منتصف عام 1995 مع تصديق العميل ● ُنفذت

# بروتوكول طبقة الوصل اآلمنة -أهداف التصميم

● قابلية التجديد

o ميكن استخدام العديد من النظم اخلوارزمية للشفرة

● شفافية املستخدم

● شفافية البيانات

o كود مصادقة الرسالة

● اإلرسال األمن بني العميل ومزود اخلدمة عند أدني مستوي -مستوي طبقة الوصل

o مواقع الربوتوكول اخلاص بروتوكول التحكم باإلرسال

● التحقق من هوية األطراف األخرى

o يُتحقق مزود اخلدمة بطريقة أتوماتيكية ويعترب العميل يف خيار من ذلك

● مستوي الكفاءة

o التخزين املؤقت للدورات

# بروتوكول طبقة الوصل اآلمنة -مراجعة الربوتوكول

● بروتوكول طبقة الوصل اآلمنة يعترب بروتوكول ذات طبقة متعددة املستويات

بروتوكول طبقة الوصل اآلمنة رسالة بنقل أجزاء البيانات إىل جمموعات قابلة لإلدارة ● يستلم

وضغط البيانات بطريقة اختيارية وتطبيق ماك والشفرات ونقل النتائج

● تشفري البيانات املُستلمة وضغطها والتحقق منها

● وإعادة جتميعها وتسليمها مبستوي عالي إىل العمالء

● التواصل مع البورت 443 بشكل تلقائي

● مهلة ختزين مؤقت لتحديد هوية اجللسة بقيمة 100 ثانية



# HTTPS بروتوكول نقل النص التشعيب اآلمن

بروتوكول نقل النص التشعيب اآلمن لتأمني التواصل عرب الشبكة احلاسوبية ● امتداد

● مُستخدم على نطاق واسع على شبكة األنرتنت

بروتوكول نقل النص التشعيب اآلمن، يُشفر بروتوكول التواصل عن طريق استخدام ● يف

(بروتوكول طبقة الوصل اآلمنة/ بروتوكول أمان طبقة النقل)

● وغالباً ما يُشري الربوتوكول إىل بروتوكول نقل النص التشعيب اآلمن عرب

طبقة الوصل اآلمنة، أو بروتوكول نقل النص التشعيب اآلمن عرب بروتوكول ● بروتوكول

أمان طبقة النقل



بروتوكول نقل النص التشعيب اآلمن يوافق احلواسب اآللية " على كود على الرسائل املستخدمة هلذا الكود لذلك ال يستطيع عن طريق استخدام "بينهم وحينئذ يعملوا على التشويش

قراءتهم. وهذا جيعل معلوماتهم أكثر أماناً من املخرتقني . نقل النص التشعيب اآلمن، إذا استطاع أي شخص بني املُرسل أحد ذلك. يستطيع فقط املُرسل واملُستلم عن طريق استخدام بروتوكول واملستلم أن يفتح الرسائل، فأنهم مازالوا ال يستوعبون

الذين هم على معرفة "بالكود"، فك تشفري الرسالة.

# مزايا استخدام بروتوكول نقل النص التشعيب اآلمن

● مصادقة املوقع اإللكرتوني الذي ميكن الوصول اليه.

● محاية خصوصية ونزاهة البيانات املتغرية عند عملية اإلرسال

● احلماية ضد منتصف هجمات الشخص