# أمن الحاسبات والمعلومات
# الفصل الثالث: علم التعمية Cryptography

**إعداد الدكتور / أسامة حسام الدين**

**كلية علوم وهندسة الحاسبات بينبع**
**جامعة طيبة**

# محتوى الفصل الثالث

- نقدم في هذا الفصل علم التعمية أو التشفير وفك التشفير

1. تعريف علم التعمية، وأنواع التشفير
2. التشفير المتماثل – التشفير بالمفتاح الخاص
3. التشفير الغير متماثل – التشفير بالمفتاح العام
4. المقارنة بين نظم التشفير المتماثلة والغير متماثلة.

# تعريف علم التعمية – التشفير وفك التشفير

- **التعمية** Cryptography هو علم بناء وتحطيم الشفرات البرمجية السرية. وعلم تطوير وصناعة واستخدام هذه الشفرات البرمجية.
- دراسة وتحليل واستنباط البيانات الأصلية من البيانات المشفرة يسمى علم استخراج المعمى Cryptanalysis. **والتشفير** Encryption هو تقنية من تقنيات التعمية، **وفك التشفير** Decryption هو من تقنيات استخراج المعمى.
- استخدم يوليوس قيصر ملك الروم شيفرة بسيطة عن طريق تغيير مكان الأحرف في النص بهدف التراسل بين جنرالات الحرب في ميدان القتال.

# تعريف التشفير

علم التشفير هو علم صناعة وكسر الشفرات السرية.

- **التشفير** يعني عملية خلط أو تشويش البيانات بطريقة منظمة بحيث لا يتمكن الأشخاص الغير مخولون من قراءة البيانات.
- تسمى البيانات المقروءة بالنص الصريح أما النسخة التي لا يسهل قراءتها تسمى النص المشفر.
- طريقة **التشفير** هي عملية تحويل النص الصريح سهل القراءة إلى نص مشفر لا يسهل قراءته. وطريقة **فك الشفرة** هي العملية العكسية أو عملية تحويل النص المشفر إلى نص صريح.

# تاريخ التشفير 1- شيفرة قيصر

استخدم يوليوس قيصر ملك الروم طريقة مشهورة باسمه تسمى شيفرة قيصر(**طريقة التعويض**)، وفيها يتم مجاورة صفين من الأحرف الهجائية. الصف الأعلى تكون فيه الحروف الأبجدية مرتبة من الألف إلى الياء أم الصف السفلي ففيه الحروف مرتبة أيضا ولكن تم تحريكها لليمين بمسافة معينة، كما نرى في الشكل تم تحريك الأحرف لليمين مسافة ثلاثة مواضع.

Alphabet shifted by 3 spaces.

**مثال:** جملة meet you in the park يتم تشفيرها إلى phhw brx lq wkh sdun، يمكن فك شفرة الجملة مرة أخرى.

# كيفية فك شيفرة قيصر

يوجد ثلاث طرق، كيف يفكر القراصنة في فك شفرة قيصر

1. تحليل عملية تكرار الأحرف
2. البحث الغاشم brute force attack
3. البحث عن الأحرف المنفردة مثل "I" و "a" والمزدوجة مثل "in" و "If" وغيرها.

# فك شيفرة قيصر بتحليل تكرار الأحرف

لوحظ أن الأحرف تتكرر في النص المشفر بنفس نمط التكرار الموجود في النص الأصلي. والحروف التي دائما ما تتكرر بكثرة هي E بمعدل 13% وحرف T بمعدل 9 % وهكذا .. انظر الجدول المرفق.

| Letter | Frequency | Ratio | Letter | Frequency | Ratio |
|---|---|---|---|---|---|
| E | 11.1607% | 56.88 | M | 3.0129% | 15.36 |
| A | 8.4966% | 43.31 | H | 3.0034% | 15.31 |
| R | 7.5809% | 38.64 | G | 2.4705% | 12.59 |
| I | 7.5448% | 38.45 | B | 2.0720% | 10.56 |
| O | 7.1635% | 36.51 | F | 1.8121% | 9.24 |
| T | 6.9509% | 35.43 | Y | 1.7779% | 9.06 |
| N | 6.6544% | 33.92 | W | 1.2899% | 6.57 |
| S | 5.7351% | 29.23 | K | 1.1016% | 5.61 |
| L | 5.4893% | 27.98 | V | 1.0074% | 5.13 |
| C | 4.5388% | 23.13 | X | 0.2902% | 1.48 |
| U | 3.6308% | 18.51 | Z | 0.2722% | 1.39 |
| D | 3.3844% | 17.25 | J | 0.1965% | 1.00 |
| P | 3.1671% | 16.14 | Q | 0.1962% | (1) |

# فك شيفرة قيصر بـ (هجمة البحث الغاشم)

- هجمة البحث الغاشم من اسمها تقوم بالبحث عن الحل بتجربة كل الاحتمالات الممكنة.
- تشبه هذه الهجمة البحث عن شخص في غرف المستشفى بفتح كل الأبواب حتى الوصول للشخص.
- تبدأ الهجمة بتجربة بالتعويض عن الحرف المجاور مباشرة فيتم استبدال A ب B و B بـ C وهكذا.
- ثم يتم تجربة التحريك بحرفين فتكون A مقابل C و B مقابل D وهكذا تستمر الخوارزمية حتى تجربة التحريك 26 حرف.

# فك شيفرة قيصر(البحث عن الأحرف المنفردة)

- ولعمل ذلك يجب البحث في الأنماط التالية
  - الكلمات القصيرة
  - الكلمات المتكررة أو الموجود فيها أنماط متكررة mission وكلمة permission
  - حروف البداية الشائعة في الاستخدام مثل a و an
  - الكلمات القصيرة المتكررة دائما مثل if و in وغيرها
  - كلما زادت المعرفة باللغة كلما سهل عملية التخمين

# تمرين عملي

wklv phvvdjh lv qrw wrr kdug wr euhdn

1. جرب بشكل يدوي
2. استخدم الأدوات المتاحة

http://www.simonsingh.net/The_Black_Chamber/caesar.html

# تاريخ التشفير 2- النقل

وفيه يتم تغيير أماكن الأحرف أو بمعنى آخر لخبطة الأحرف، مثلا يتم تنظيم النص في صورة صفوف وأعمدة ثم يتم اختيار الأعمدة كأنها الكلمات المشفرة، وبذلك يتم تفادي عملية تكرار الأحرف الموجودة في شيفرة قيصر.

**مثال:** النص I HATE MY BOSS OSAMA يتم تشفيرها بتحويلها مثلا إلى أربعة أعمدة كما بالشكل، ويكون النص المشفر هو الكلمات في الأعمدة IEOS HMSA AYSM TBOA.

| | | | |
|---|---|---|---|
| I | H | A | T |
| E | M | Y | B |
| O | S | S | O |
| S | A | M | A |

# تاريخ التشفير 3 ـ غلاف المرة الواحدة

- في غلاف المرة الواحدة One-time pad يتم دمج النص الصريح مع مفتاح سري عشوائي يستخدم مرة واحدة فقط لعمل حرف جديد. ثم يتم إجراء عملية منطقية تسمى XOR بين الحرف الجديد وبين النص الصريح للحصول على النص المشفر كما هو موجود بالصورة.

النص الأصلي: 10110010111001
المفتاح: 11010001010100
النص المشفر: 01100011101101

# أنواع التشفير –1 شيفرة الكتل Block

تقوم شيفرة الكتل بتحويل كتلة من البتات بطول ثابت إلى كتلة معروفة الطول مثلا 64 بت أو 128 بت. وحجم الكتلة هنا يعبر عن كمية البيانات التي يتم تشفيرها في المرة الواحدة.

- (دياس DES) هي خوارزمية متماثلة تقوم بتشفير كتلة بحجم 64 بت مستخدمة مفتاح بطول 56 بت.

# أنواع التشفير –2 شيفرة التدفق Stream

تقوم شيفرة التدفق بتشفير النص الصريح بأخذ بايت واحد أو بت واحد في المرة الواحدة.

- شيفرة التدفق ممكن أن تكون أسرع بكثير من شيفرة الكتل، وعادة لا يتم زيادة حجم الرسالة، حيث أنه يمكن تشفير عدد اعتباطي من البتات.
- A5 هي شيفرة تدفقية تعطي خصوصية للاتصال الصوتي حيث تقوم بتشفير جميع الاتصالات الصوتية

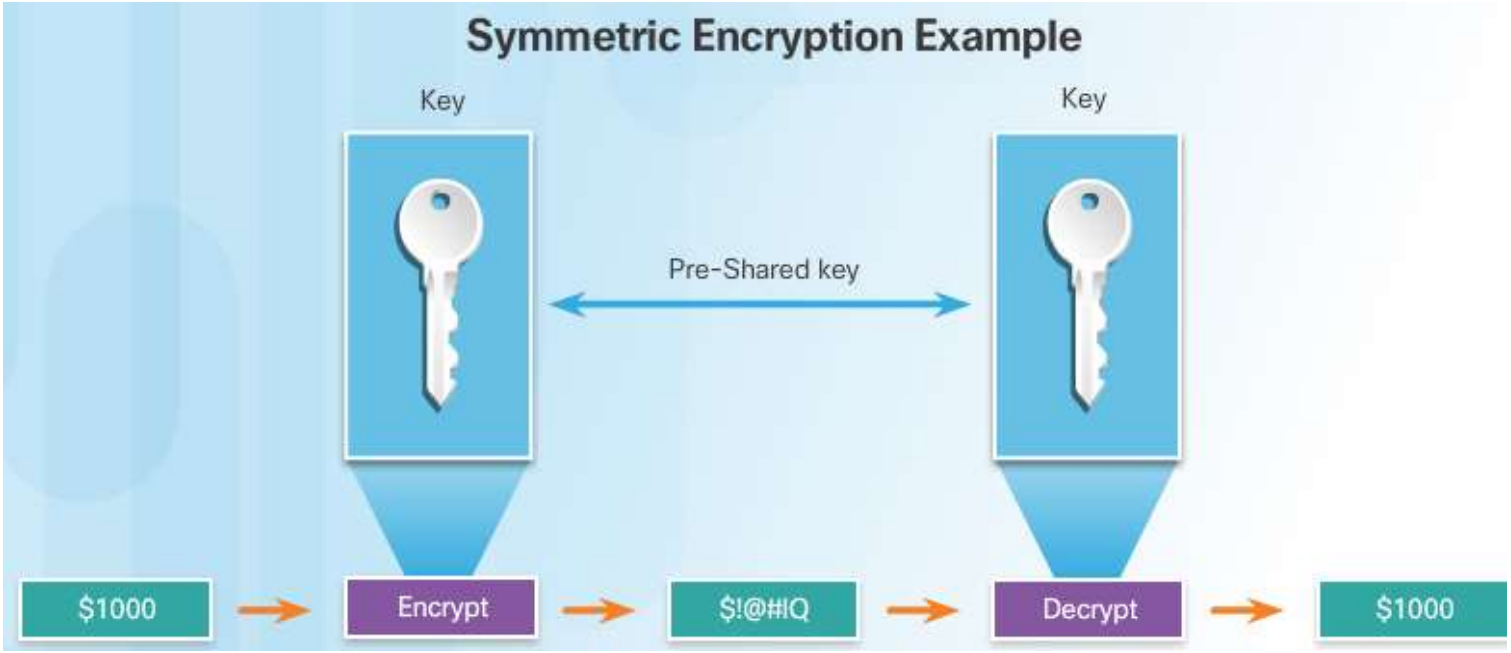
# فئات التشفير

يوجد منهاجين لتأكيد سرية البيانات عند استخدام التشفير

- **المنهاج الأول** هو حماية خوارزمية التشفير. فإذا كانت سرية الخوارزمية تعتمد اعتمادا كليا على الخوارزمية نفسها، فيجب حمايتها بشتى الطرق الممكنة
- **المنهاج الثاني** هو حماية مفاتيح التشفير. مع نظم التشفير الحديثة، تكون الخوارزمية معروفة للجميع. ومفاتيح التشفير هي التي تؤكد على سرية البيانات. ومفاتيح التشفير هي كلمات المرور التي تكون جزء من المدخلات لأي خوارزمية تشفير والجزء الثاني يكون النص الصريح المراد تشفيره

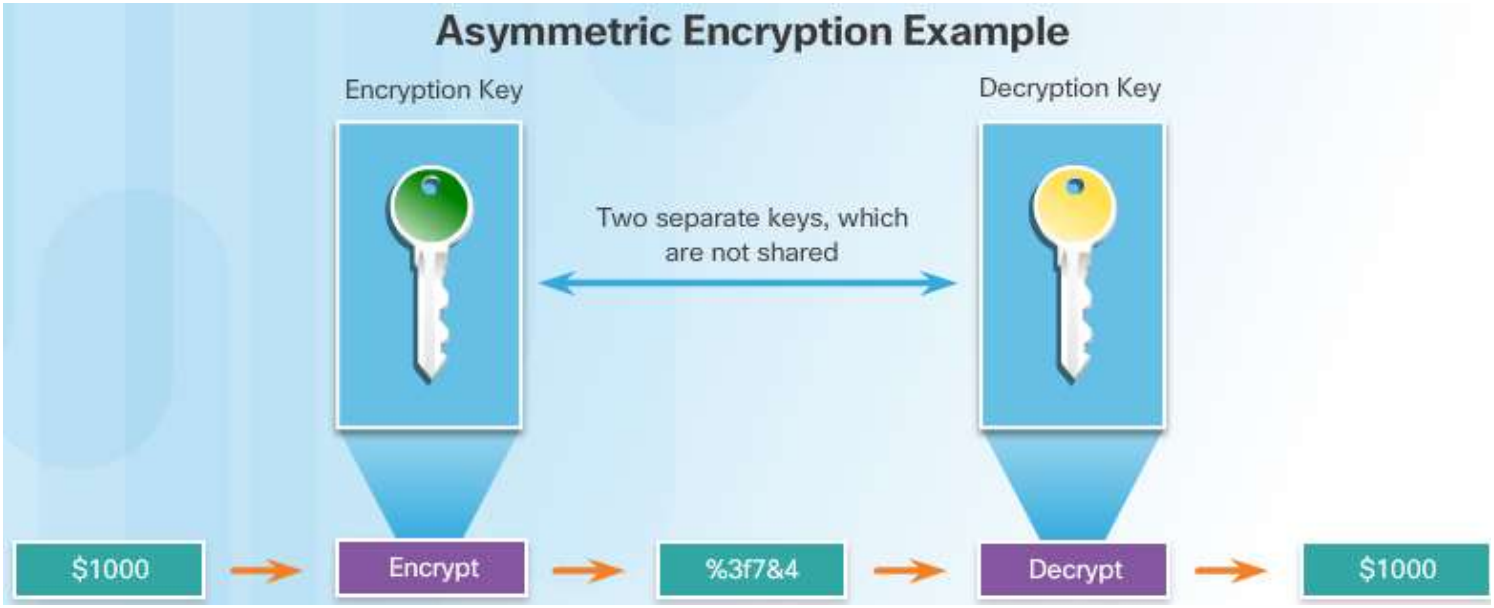
# فئات التشفير – التشفير المتماثل

وهذه الخوارزميات تستخدم نفس المفتاح المشترك في عمليتي التشفير وفك التشفير. ويجب أن يتم تشارك المفتاح بين المرسل والمستقبل قبل البدء في أي عملية اتصال.



# فئات التشفير – التشفير الغير متماثل

تستخدم الخوارزميات الغير متماثلة مفتاح للتشفير ومفتاح مختلف لفك التشفير. المفتاح الأول يكون مفتاح عام والثاني يكون مفتاح خاص.



# فئات التشفير – التشفير المتماثل

تسمى أيضا هذه الطريقة طريقة "التشفير بالمفتاح الخاص".

- يتم استخدام مفتاح واحد فقط. فإليسا وبوب يمتلكان نسختين من نفس المفتاح لقفل واحد.
- تقوم إليسا بكتابة الرسالة السرية وتضع الرسالة في صندوق صغير والذي تقوم بغلقة بالقفل.
- وعندما يستقبل بوب الصندوق، يستخدم نفس مفتاح اليسا لفك القفل واستخراج الرسالة. ويمكن لبوب أن يرسل ردا سريا إلى إليسا باستخدام نفس الصندوق
- إذا أراد بوب مراسلة العديد من الفتيات بشكل سري سيحتاج إلى عدد من المفاتيح يساوي عدد الفتيات. وستظهر حينها مشكلة إدارة مفاتيح المراسلة.

# فئات التشفير - خوارزميات التشفير المتماثل

بعض من الطرق الشائعة والقياسية للتشفير تستخدم التشفير المتماثل مثل:

**الأولى: 3DES أو دياس الثلاثي**: دياس(DES) هو نظام تشفير كتلي متماثل يستخدم كتل بحجم 64 بت ومفتاح بطول 56 بت. حيث يأخذ الكتلة بحجم 64 بت من النص الصريح ويحولها إلى كتلة مشفرة بحجم 64 بت أيضا. ودياس الثلاثي(3DES) يقوم بتشفير البيانات ثلاث مرات باستخدام دياس.

**ودورات دياس التشفيرية الثلاث هي كالاتي:**

- يتم تشفير البيانات باستخدام أول دياس
- يتم فك التشفير باستخدام ثاني دياس
- يتم إعادة التشفير مرة أخرى باستخدام ثالث دياس.

والعملية العكسية تقوم بفك تشفير النص.

# فئات التشفير - خوارزميات التشفير المتماثل

**الثانية: إياس AES:** معيار التشفير المتقدم (إياس) له حجم كتله ثابت بطول 128 بت ومفتاح بطول 128 و 192 و 256 بت. أقر المعهد الوطني للمعايير والتكنولوجيا (نيست) خوارزمية إياس في ديسمبر 2001.

- إياس أسرع من دياس ودياس الثلاثي، ولذا فإنه يعطي حلولا لكل من التطبيقات البرمجية والعتاد المستخدم كجدار ناري أو موَجه

**أنواع أخرى:** ويوجد أنواع أخرى من طرق التشفير الكتلي مثل سكيب جاك Skipjack وتم تطويره من قبل وكالة الفضاء الأمريكية (ناسا)، ويوجد أيضا بلوفيش Blowfish و توفيش Twofish و إيديا (IDEA). إيديا جاء لاستبدال دياس ويستخدمه برنامج PGP للخصوصية. وبرنامج PGP يعطي خصوصية وتوثيق لبيانات الاتصال.

# تمرين عملي

- استخدم أداة التشفير الكتلي AES الموجودة على الرابط http://aesencryption.net/ في عمل الآتي:
- أكتب رسالة لزميلك، قم بتشفيرها باستخدام شيفرة إياس AES
- ارسل الرسالة المشفرة لزميلك
- أطلب من زميلك الدخول على الرابط وفتح الرسالة وفك تشفيرها.
- تأكد من أن زميلك حصل على الرسالة بشكل سليم.

# فئات التشفير – التشفير الغير متماثل

وتسمى أيضا عملية التشفير بالمفتاح العام، تستخدم مفتاحا للتشفير مختلفا عن مفتاح فك التشفير.

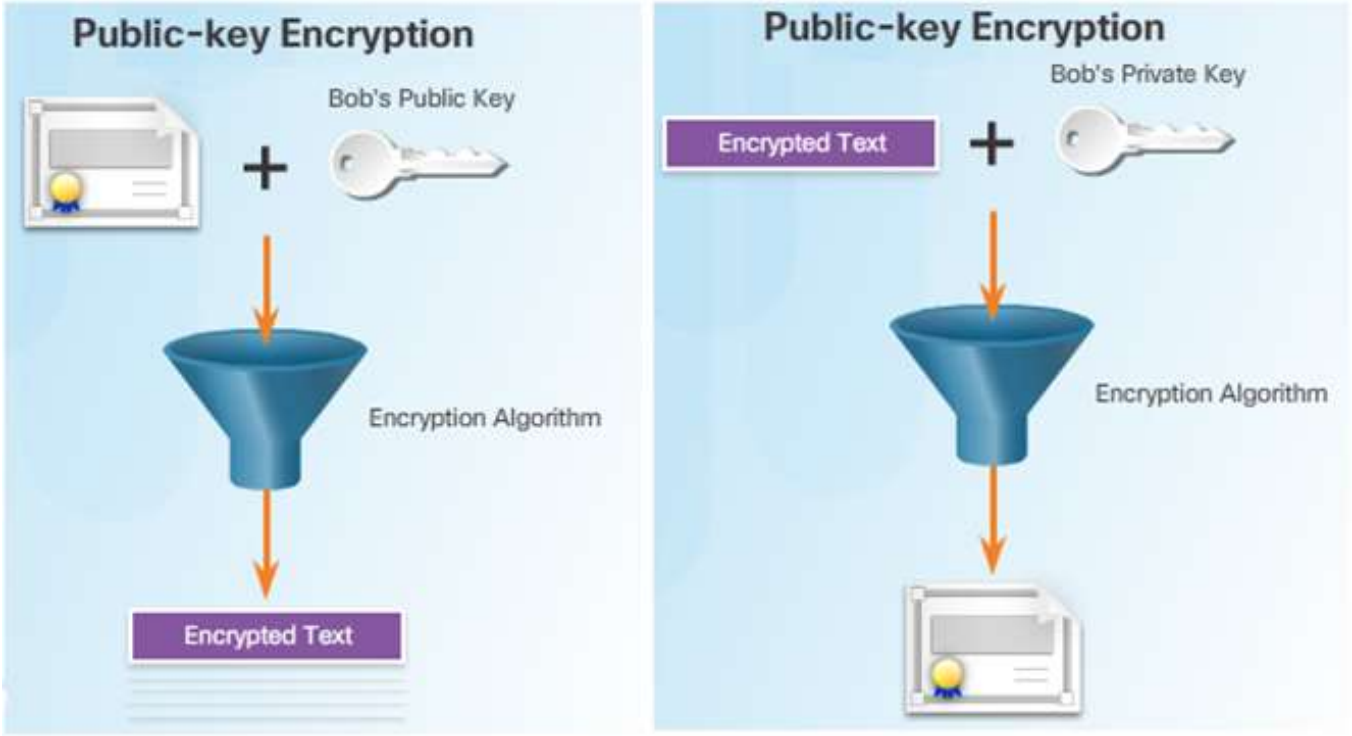
- يكون لدى بوب قفل و مفتاح مختلف عن القفل والمفتاح الذين يخصان إليسا.
- فإذا أرادت إليسا إرسال رسالة سرية لبوب، يجب أن تتصل به ليرسل لها قفله مفتوحا، يقوم بوب بإرسال قفله المفتوح لإليسا ولكن يحتفظ بالمفتاح.
- وعندما تستقبل إليسا القفل المفتوح، تقوم بكتابة الرسالة السرية ووضعها في الصندوق الصغير وتضع أيضا قفلها المفتوح في الصندوق ولكن تحتفظ بمفتاحها الخاص ثم تغلق الصندوق بقفل بوب.

# فئات التشفير – التشفير الغير متماثل

في الشكل إليسا تتقدم بطلب للحصول على مفتاح بوب العام (القفل في المثال).

# فئات التشفير – التشفير الغير متماثل

في الشكل تقوم إليسا باستخدام مفتاح بوب العام لتشفير الرسالة باستخدام خوارزمية متفق عليها. تقوم إليسا بإرسال الرسالة المشفرة لبوب، ثم يقوم بوب باستخدام مفتاحه الخاص لفك تشفير الرسالة



# فئات التشفير - خوارزميات التشفير الغير متماثل

- **RSA ريشاد :** يتم استخدام حاصل ضرب عددين أوليين كبيرين بطول ثابت بين 100 و 200 رقم. تستخدم متصفحات الانترنت خوارزمية ريشاد لإقامة اتصال آمن.
- **ديفي هيلمان:** يستخدم طريقة إلكترونية لتبادل ومشاركة المفاتيح السرية. والبروتوكولات SSLو TSLو SSHو IPSecجميعها تستخدم خوارزمية ديفي هيلمان.
- **الجمل:** يستخدم معيار الحكومة الأمريكية للبصمات الرقمية. هذه الخوارزمية مفتوحة المصدر إذ لا يملك أحد براءة اختراع لها.
- **تشفير المنحنى البيضاوي**: يستخدم المنحنيات البيضاوية كجزء من الخوارزمية. ووكالة الأمن الوطني NSA في أمريكا تستخدم تشفير المنحنى البيضاوي لعمل بصمات رقمية ولتبادل المفاتيح السرية.

# إدارة المفاتيح

- تتكون إدارة المفاتيح من العمليات التالية، التخليق، والتبادل، والتخزين، والاستخدام، واستبدال المفاتيح المستخدمة في خوارزميات التشفير.
- إن أصعب المهام في نظام التشفير هي "إدارة المفاتيح". فمعظم نظم التشفير تفشل بسبب خطأ في عملية إدارة المفاتيح.
- هناك مصطلحان هامان يصفان المفاتيح
  - **طول المفتاح** – يسمى أيضا حجم المفتاح، ويقاس بالبت
  - **فضاء المفتاح** – هو عدد التباديل الممكنة المستخرجة من مفتاح بطول ثابت.

كلما زاد طول المفتاح، كلما زاد فضاء المفتاح زيادة مضطردة.
وفضاء المفتاح لخوارزمية معينة هو مجموعة القيم الممكنة لذلك المفتاح. المفاتيح الأطول أكثر أمانا، وعلى الرغم من ذلك، فالمفاتيح الطويلة تستهلك الموارد.

# مراحل إدارة المفاتيح

1. تخليق المفتاح: يتم عادة ميكنة عملية تخليق المفاتيح ولا يتم تركها للمستخدم
2. التحقق من المفتاح: وتسمى أيضا التحقق من جودة المفتاح. بعض المفاتيح أفضل من الأخرى. على سبيل المثال استخدام مفتاح بطول 0 و 25 في شيفرة قيصر لن يشفر النص ولذلك يجب أن يستبعد هذين المفتاحين.
3. تبادل المفتاح: نظم إدارة المفاتيح يجب أن توجد آلية تبادل للمفاتيح والتي تسمح بالاتفاق على التراسل السري بين المرسل والمستقبل، وعادة ما يتم التراسل في وسط غير آمن.

# مراحل إدارة المفاتيح

4. تخزين المفتاح: نظم التشغيل الحديثة متعددة المستخدمين تستخدم نظم التشفير وتخزن المفاتيح في الذاكرة. وهذا يمثل مشكلة
5. عمر المفتاح: يجب أن يتم استخدام مفتاح بعمر قصير حتى تزيد سرية الشيفرات الاعتيادية.
6. إلغاء وتدمير المفتاح: عملية الإلغاء تعني إخبار كل أطراف الاتصال بأن مفتاح معين تم كشفه ولا يجب استخدامه مرة أخرى. أما عملية تدمير المفتاح فتقوم بإزالة المفتاح بحيث لا يتم ترك أثر يمكن تتبعه من قبل القراصنة.

# مقارنة أنواع التشفير

| التشفير المتماثل والغير متماثل | |
|---|---|
| **التشفير المتماثل** | **التشفير الغير متماثل** |
| مشهور باسم خوارزميات المفاتيح الخاصة السرية والمشتركة | مشهور باسم خوارزميات المفاتيح العامة |
| طول المفتاح عادة يتراوح بين 80 و 256 بت | طول المفتاح يتراوح بين 512 و 4096 بت |
| المرسل والمستقبل يجب أن يتشاركان نفس المفتاح | المرسل والمستقبل لا يتشاركان في مفتاح محدد |
| خوارزمياته دائما سريعة (سرعة وسط النقل) لأن الخوارزمية تعتمد على عمليات حسابية بسيطة. | خوارزمياته بطيئة نسبيا لأنها تعتمد على عمليات حسابية أكثر تعقيدا. |
| من الأمثلة عليه، دياس، إياس، إياس الثلاثي، إديا، بلوفيش | من الأمثلة عليه، ريشاد RSA و الجمل و المنحنى البيضاوي |

# الأسئلة