الجمهورية العربية السورية
جامعة قرطبة الخاصة
كلية الهندسة / تكنولوجيا هندسة الاتصالات والمعلومات

ملخص محاضرة خاصة بمقرر مادة
"وثوقية وأمن المعلومات"
" تطبيقات وثوقية وأمن المعلومات 2"
للفصل الثاني للعام الدراسي 2020/2019
بعنوان:

معايير التشفير الرقمية

Digital Encryption Standard (DES, 3DES and AES)

I. ما هي معايير التشفير Encryption Standard:

يمكن تصنيف معايير أو أنظمة التشفير إلى نوعين رئيسين:

1- تشفير رقمي Digital Encryption

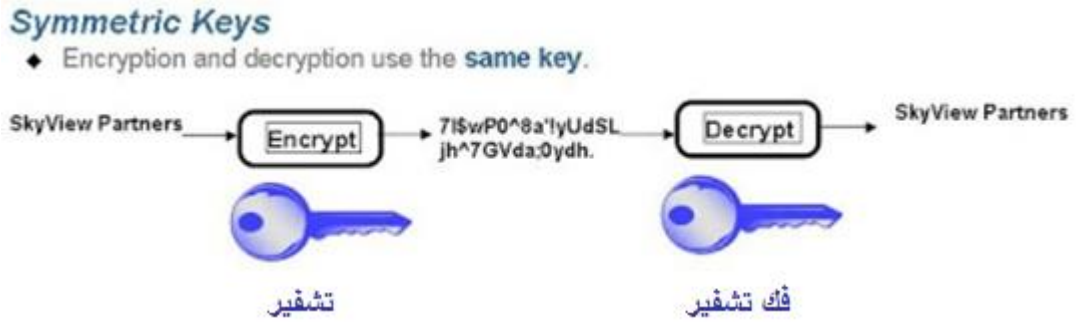
2- تشفير غير رقمي Non Digital Encryption

I. معايير التشفير الرقمية Digital Encryption Standard:

- تصنف كأنظمة تشفير متماثلة Symmetric Encryption

- تستخدم مفاتيح تشفير متماثلة Symmetric Keys:

نفس المفتاح (مفتاح واحد) يستخدم للتشفير Encryption ولفك التشفير Decryption : شكل (1)



شكل (1)

- **أمثلة:**

- الغوريتم التشفير DES
- الغوريتم التشفير 3DES
- الغوريتم التشفير AES

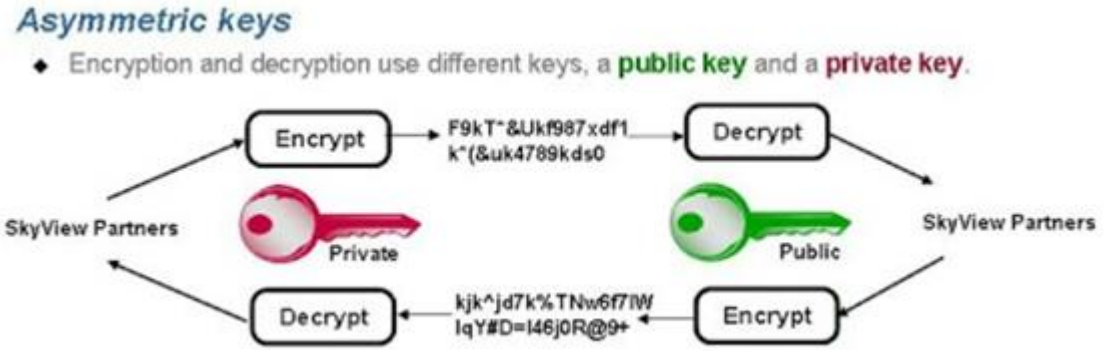
II. معايير التشفير التقليدية Classical Encryption Standard:

- تصنف كأنظمة تشفير غير متماثلة Asymmetric Encryption

- تستخدم مفاتيح تشفير متماثلة Asymmetric Keys:

تستخدم مفتاحين:

1. (مفتاح عام public key) للتشفير Encryption
2. (مفتاح خاص private key) لفك التشفير Decryption: شكل (2)



شكل (2)

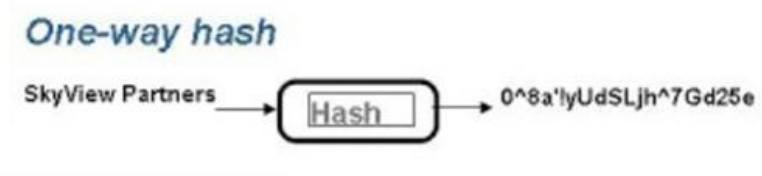
- **أمثلة:**

- الغوريتم التشفير RSA
- الغوريتم التشفير Elliptic
- الغوريتم التشفير Curve

III. الغوريتم التشفير هاش* Hash Encryption Algorithm:

- يصنف كأنظمة تشفير باتجاه واحد One-Way Hash

- لا يستخدم مفاتيح تشفيرNo Keys : شكل (3)



شكل (3)

- **أمثلة:**

- الغوريتم هاش SHA-1
- الغوريتم هاش SHA-256
- الغوريتم هاش MD5

*) الغوريتم التشفير هاش يُلحق بأنواع التشفير كنوع ثالث!

1. معيار التشفير الرقمي Digital Encryption Standard (DES):

معيار تشفير البيانات (DES) هو تشفير مفتاح متماثل بطول 56 bits.

تم تطويره من قبل شركة IBM عام 1975 نشره المعهد الوطني للمعايير والتكنولوجيا NIST. تم تعديله عدة مرات بطلب من وكالة الأمن القومي الأمريكية NSA.

- **تصدع معيار التشفير الرقمي Cracked (DES):**

- عام 1997 تم اختراق رسالة مشفرة بمعيار التشفيرDES-Encrypted message خلال 3 أيام

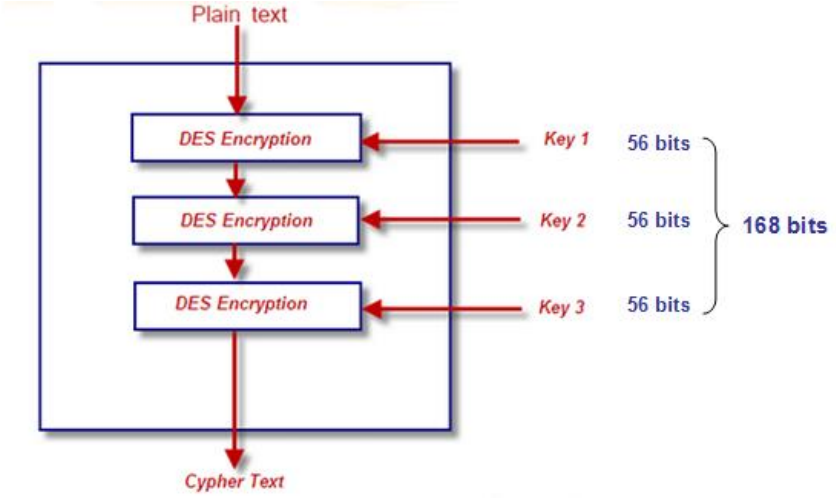
- عام 1998 قامت شبكة مؤلفة من 10000 حاسب باختراق DES-Encrypted message بأقل من يوم واحد

2. معيار التشفير الرقمي الثلاثي Tribble Digital Encryption Standard (3DES):

- معيار تشفير البيانات (3DES) هو تشفير مفتاح متماثل بطول 56 bits أيضاً.

- في حين يستخدم DES مفتاح **واحد** للتشفير وفك التشفير ؛ يمكن لـ 3DES استخدام **مفتاحين أو ثلاثة** بطول مكافئ 168 bits لعمل جولات إضافية من التشفير: الشكل (4)

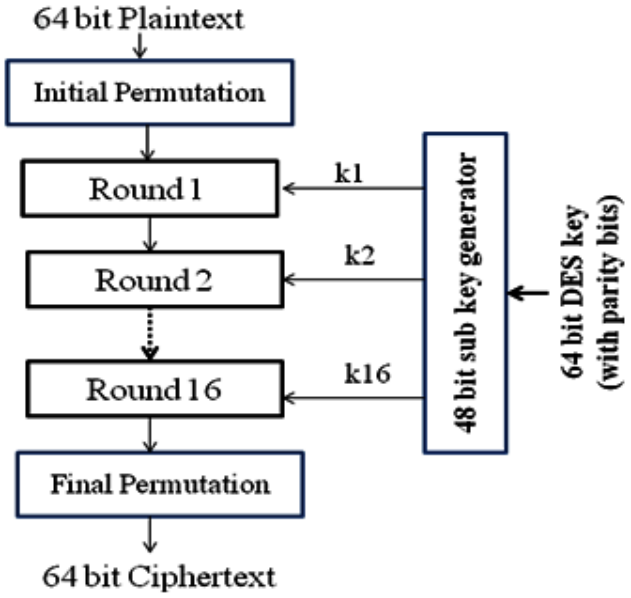
- **مبدأ عمل الغوريتم التشفير 3DES:** هو **تكرار** الغوريتم التشفير **DES ثلاث مرات (جولات)** بشكل **متعاقب** بحيث يتم استخدام المفتاح **Key1** في الجولة الأولى لتشفير النص الأصلي (Plain text) للحصول على النص المشفر **Cipher-text1**. ثم يتم استخدام المفتاح **Key2** في الجولة الثانية لتشفير النص المشفر **Cipher-text1** كنص أصلي Plain-text للحصول على النص المشفر **Cipher-text2** . ثم يتم استخدام المفتاح **Key3** في الجولة الثالثة لتشفير النص المشفر **Cipher-text2** كنص أصلي Plain-text للحصول على النص المشفر **Cypher-text3** كخرج نهائي (Cipher Text).



شكل (4)

- **ملاحظة:**

للحصول على وثوقية أكبر وبغية تخفيض زمن الاختراق Cracked time يمكن تكرار الغوريتم التشفير DES بشكل متعاقب أكثر من ثلاث (جولات) لغاية 16 جولة و يتم ذلك باستخدام 16 مفتاح كل منها بطول 64 bits كما هو مبين في الشكل (5):



شكل (5)

كما يلاحظ في الشكل (5) أيضاً استخدام مولد مفتاح جزئي Sub-key generator بطول 64 bits لتعزيز الوثوقية عند توليد المفاتيح المستخدمة.

3. معيار التشفير الرقمي المتقدم (AES) Advanced Encryption Standard:

- معيار تشفير البيانات الرقمي المتقدم أو المطور (AES) هو تشفير مفتاح متماثل بطول 128 bits.
- تعتبر خوارزمية AES تطويراً لخوارزمية DES و 3DES.
- تم تطويره بطلب من المعهد الوطني للمعايير والتكنولوجيا NIST.
- في عام 2001 تم نشره تحت اسم الغوريتم التشفير Rijndael.
- الغوريتم التشفير Rijndael يعرف بلوكات Block size مختلفة الحجم ومفاتيح بأطوال مختلفة من مضاعفات 32 bits.
- بينما الغوريتم التشفير AES المطور من Rijndael يعرف بلوكات تشفير Block size ثابتة الحجم 128 bits لكن بمفاتيح بأطوال 128 bits و192 bits و256 bits.
- يعتبر AES الطريقة الأكثر أماناً للتشفير وذلك بسبب **طول مفتاح** التشفير.

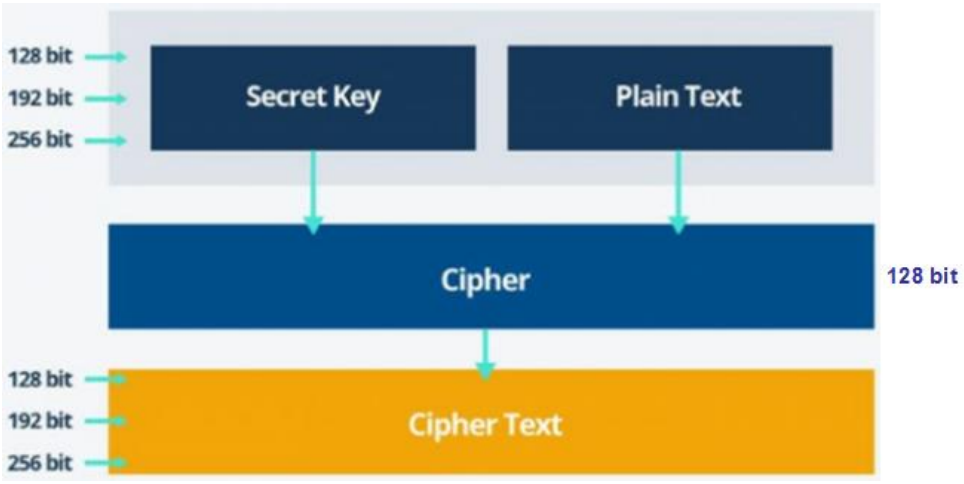
• مبدأ عمل الغوريتم التشفير AES:

يتكون بناء معيار التشفير المتقدم AES وفق ثلاث شفرات رئيسية: AES-128 و AES-192 و AES-256.

يتم تشفير Encryption وفك تشفير Decryption البيانات في قطع Block بحجم ثابت 128 bit باستخدام مفاتيح التشفير مختلفة 128 bits أو 192 bits أو 256 bits.

تستخدم جميع شفرات التشفير المتماثل المفتاح نفسه لتشفير البيانات وفك تشفيرها ، مما يعني أنه يجب أن يكون لكل من المرسل والمستقبل نفس المفتاح.

يُنظر إلى كل طول مفتاح على أنه كافٍ لحماية البيانات. تحتوي مفاتيح 128 bits على 10 جولات، وتحتوي مفاتيح 192 bits على 12 بينما تحتوي مفاتيح 256 bits على 14 جولة. الشكل (6):



شكل (6)

- **ملاحظة:**

باعتبار أن بلوك التشفير ثابت الطول نلاحظ أن طول المفتاح هو الذي يمنح اسم صنف الغوريتم التشفير AES كما هو مبين بالجدول:

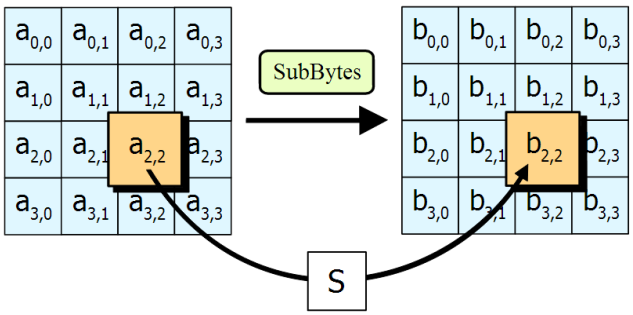
AES	Block size (bits)	Key length (bits)	Cipher text (bits)
AES-128	128	128	128
AES-192	128	192	192
AES-256	128	256	256

- **خطوات عملية التشفير المتقدم AES steps:**

1. The SubBytes step

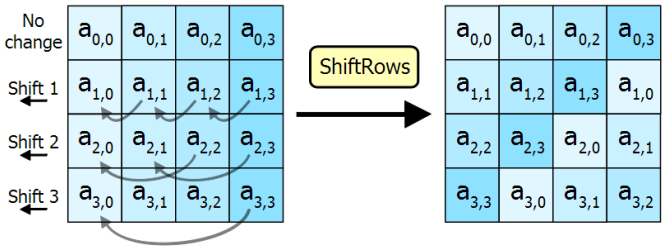
1. استبدال المعلومات Substituting the information: باستخدام جدول الاستبدال (وهو عبارة عن مصفوفة رباعية 4x4 يمثل كل عنصر فيها byte وبالتالي يتكون لدينا 16 bytes)

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$



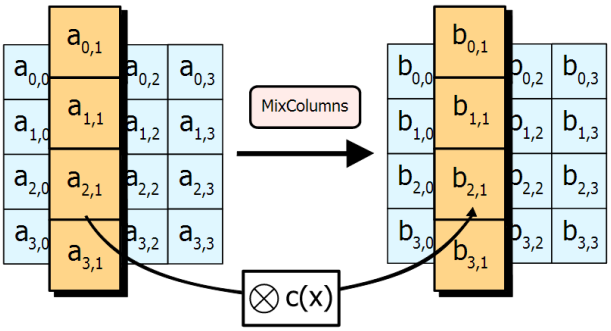
2. The ShiftRows step

2. تغيير تحويل صفوف البيانات Transmutation changes data rows:



3. The MixColumns step

3. تغيير تحويل صفوف البيانات Shifts columns: الشكل (1)

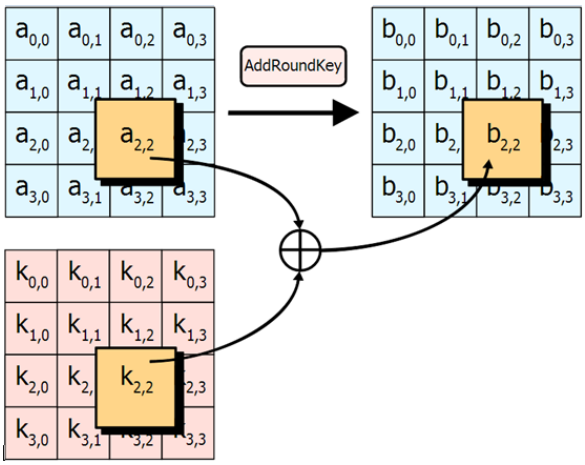


In the MixColumns step, each column of the state is multiplied with a fixed polynomial

$$\begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix} \qquad 0 \le j \le 3$$

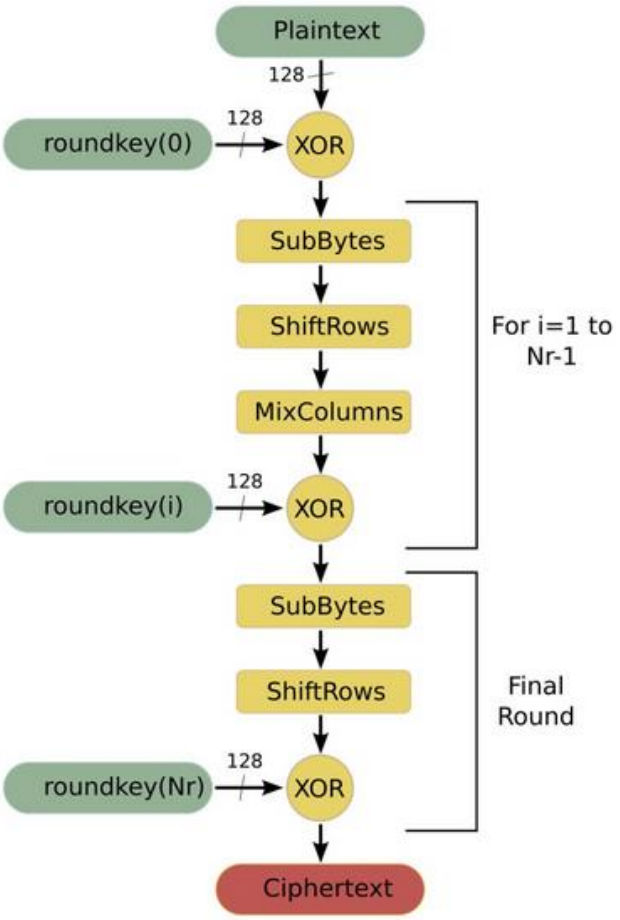
4. تنفيذ عملية XOR Apply XOR process على كل عمود باستخدام جزء مختلف من مفتاح التشفير.

5. تنفيذ عملية تكرار جولات Apply Round process. كلما كان مفتاح التشفير أطول ، زادت الحاجة لمزيد من الجولات.



- **المخطط الانسيابي لعملية التشفير المتقدم Flowchart of AES steps:**

يبين الشكل (7) المخطط الانسيابي Flowchart لعملية التشفير المتقدم AES ويلاحظ فيه أن الخطوات الثلاث الأساسية (SubBytes وShiftRows وMixColumns) تنفذ بالنسبة لكل جولات التشفير باستثناء الجولة الأخيرة عمليتي SubBytes وShiftRows فقط.



شكل (7)

- **مثال: تشفير وفك التشفير الغوريتم AES-256 في بيئة آندرويد***

Example: AES-256 Encryption & Decryption in Android

1). First step of the code is generating a random **Secretkey.** We've used **KeyGenerator** (by setting *keysize* 256) to generate the **Secretkey**:

```
KeyGenerator keyGenerator;
SecretKey secretKey;
keyGenerator = KeyGenerator.getInstance("AES");
keyGenerator.init(256);
secretKey = keyGenerator.generateKey();
```

2). Secondly, I've used IV,Initialization Vector in my code. (This is optional in AES Encryption but better to use):

```
byte[] IV = new byte[16];
SecureRandom random;
random = new SecureRandom();
random.nextBytes(IV);
```

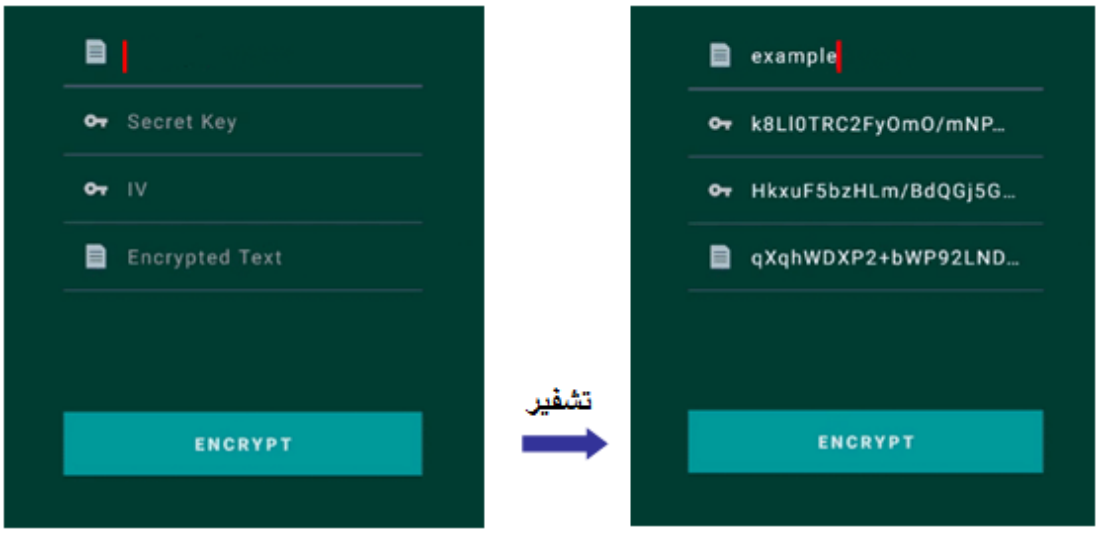
3). After defining two important parameter, step forward to **coding** functions:

a. Encrypt function

```
public static byte[] encrypt(byte[] plaintext, SecretKey key, byte[]
IV) throws Exception
{
    Cipher cipher = Cipher.getInstance("AES");
    SecretKeySpec keySpec = new SecretKeySpec(key.getEncoded(),
"AES");
    IvParameterSpec ivSpec = new IvParameterSpec(IV);
    cipher.init(Cipher.ENCRYPT_MODE, keySpec, ivSpec);
    byte[] cipherText = cipher.doFinal(plaintext);
    return cipherText;
}
```

b. Decrypt function

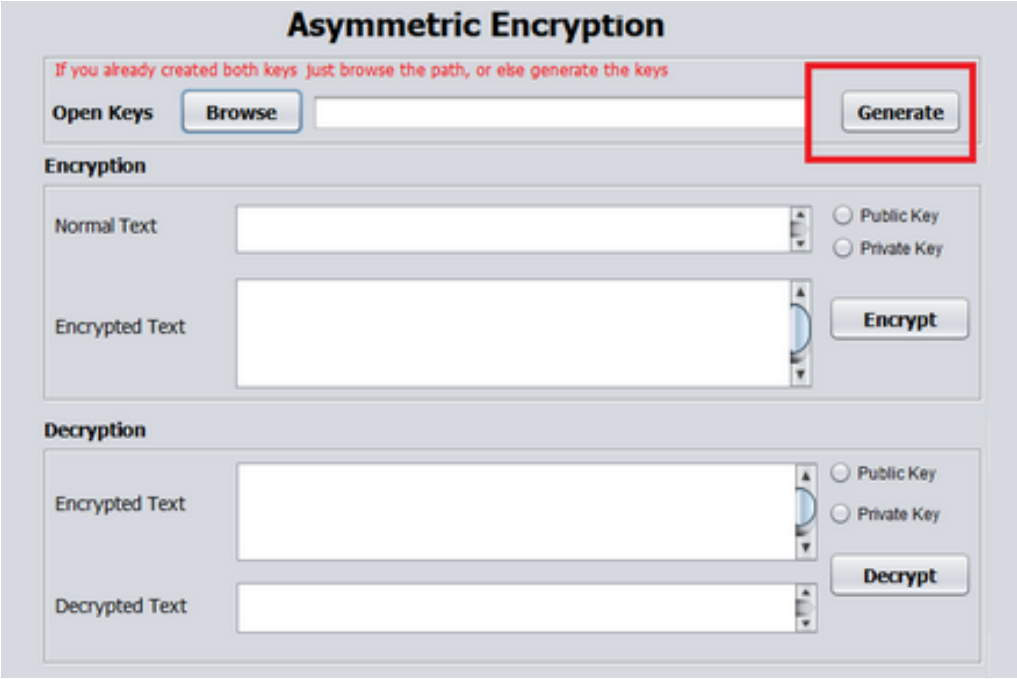
```
public static String decrypt(byte[] cipherText, SecretKey key, byte[]
IV)
{
    try {
        Cipher cipher = Cipher.getInstance("AES");
        SecretKeySpec keySpec = new SecretKeySpec(key.getEncoded(),
"AES");
        IvParameterSpec ivSpec = new IvParameterSpec(IV);
        cipher.init(Cipher.DECRYPT_MODE, keySpec, ivSpec);
        byte[] decryptedText = cipher.doFinal(cipherText);
        return new String(decryptedText);
    } catch (Exception e) {
        e.printStackTrace();
    }
    return null;
}
```



*) المثال للاطلاع فقط!

ملاحظة:

يبين الشكل (8) واجهة أحد برمجيات التي يتم من خلالها اختيار نوع الغوريتم التشفير بالإضافة إلى اختيار حجم بلوك التشفيرCipher Block size وطول مفتاح التشفير Key length ومن ثم توليده إلى ما هنالك من العمليات المتممة كاختيار عدد جولات التكرار والنسخ والحفظ:



شكل (8)

***

حلب 2020/4/20

مع كل التمنيات بالنجاح والتوفيق

مدرس المقرر: **الدكتور حسن مسلماني**