



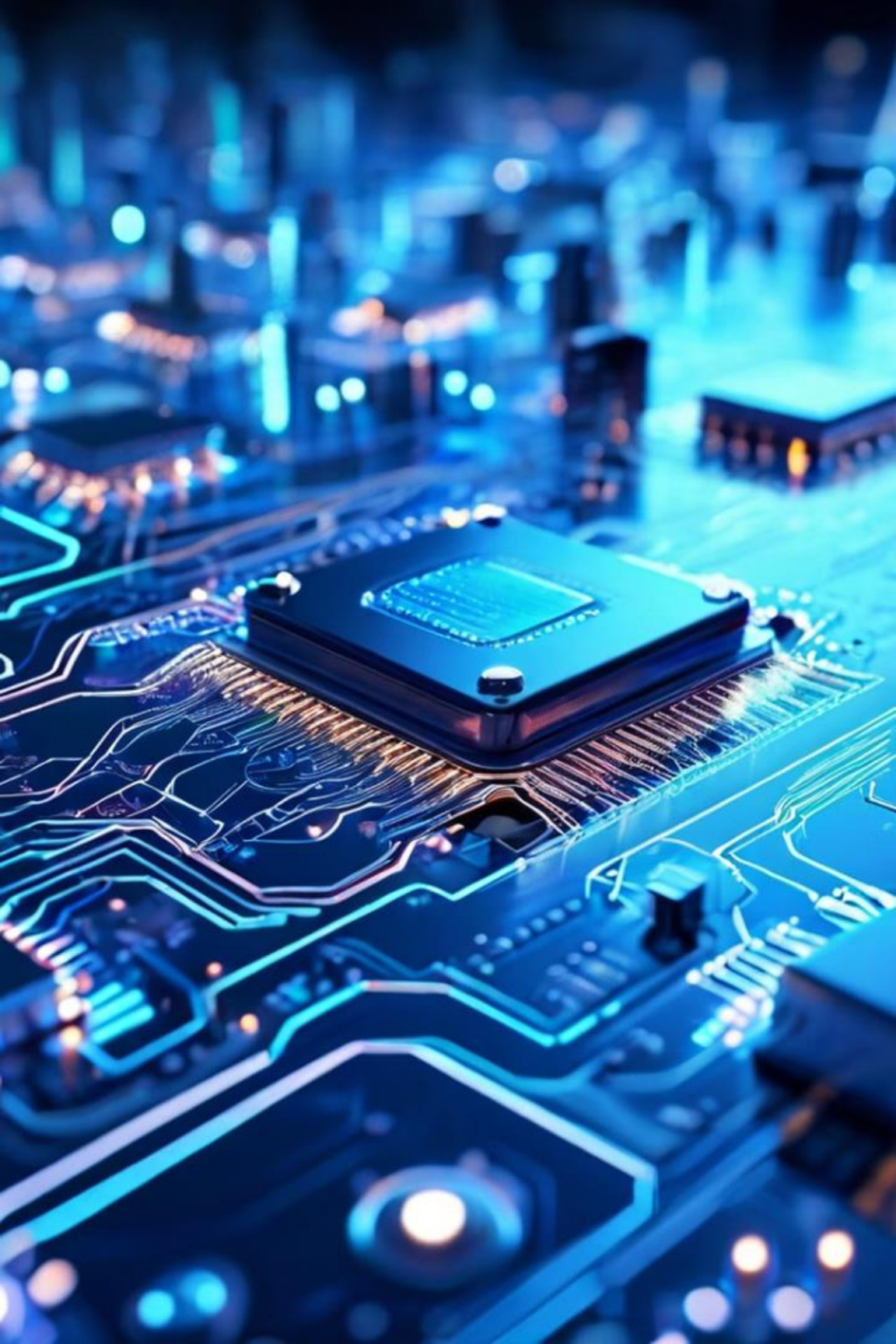
مقدمة عن تشفير البيانات

**Level 4 IT**

**IBB Un**

by

**Eng:Eissa AL-gumaei**



# علم التشفير

التشفير هو فنّ تحويل البيانات إلى شكل غير مفهوم لمنع الوصول غير المصرح به .يوفر التشفير حماية قوية للبيانات، مما يجعلها آمنة من أعين المتطفلين.





# أهداف نظام التشفير

الهدف الرئيسي من التشفير هو ضمان أمن البيانات، وتوفير السرية، والصلاحيّة، والتكاملية، وعدم التكرار.

## 1 الصلاحيّة

التأكد من صحة مصدر الرسالة ومنع التزوير.

## 2 السرية

ضمان عدم وصول غير المصرح لهم إلى المعلومات.

## 3 عدم التكرار

ضمان عدم إنكار المرسل لرسالته.

## 4 التكاملية

منع التلاعب بالبيانات، سواء أُو الحذف.

# مكونات نظام التشفير

الهدف الرئيسي من التشفير هو ضمان أمن البيانات، وتوفير السرية، والصلاحيه، والتكاملية، وعدم التكرار.

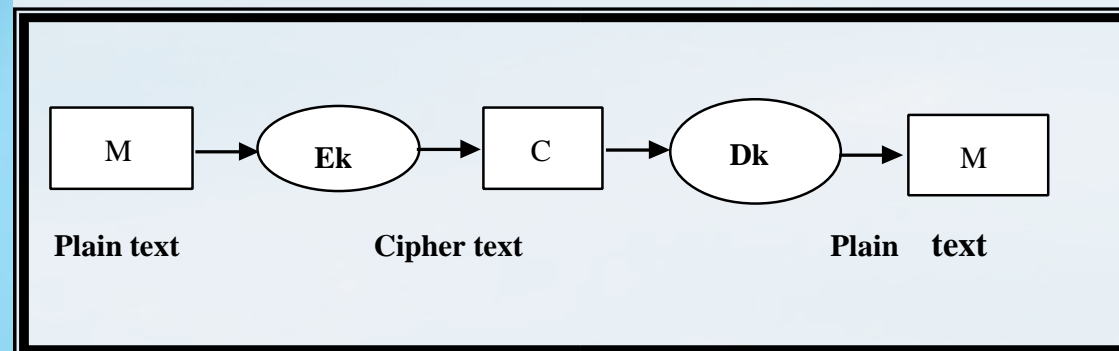
1 plaintext

2 Ciphertext

3 مفتاح Key

4 خوارزمية التشفير Encryption

5 خوارزمية فك التشفير Dk



# تطبيقات التشفير في الحياة اليومية



## المعاملات عبر الإنترنت

ضمان أمان معلومات الدفع والبيانات



## شبكات الواي فاي

توفير اتصال آمن بين الأجهزة



## البريد الإلكتروني

حماية الرسائل من الاختراق والتجسس



## أجهزة الكمبيوتر

حماية البيانات الشخصية من الوصول  
المصرح به





# أنواع خوارزميات التشفير

1

## التشفير المتماثل

يستخدم نفس المفتاح للتشفير وفك  
يُستخدم في مهام مثل .التشفير  
تشفير الملفات.

2

## التشفير غير المتماثل

مفتاح :يستخدم مفتاحين مختلفين  
للتشفير ومفتاح خاص لفك التشفير  
يُستخدم في مهام مثل التوقيع الرقمي



# أنواع خوارزميات التشفير

1

## التشفير المتماثل

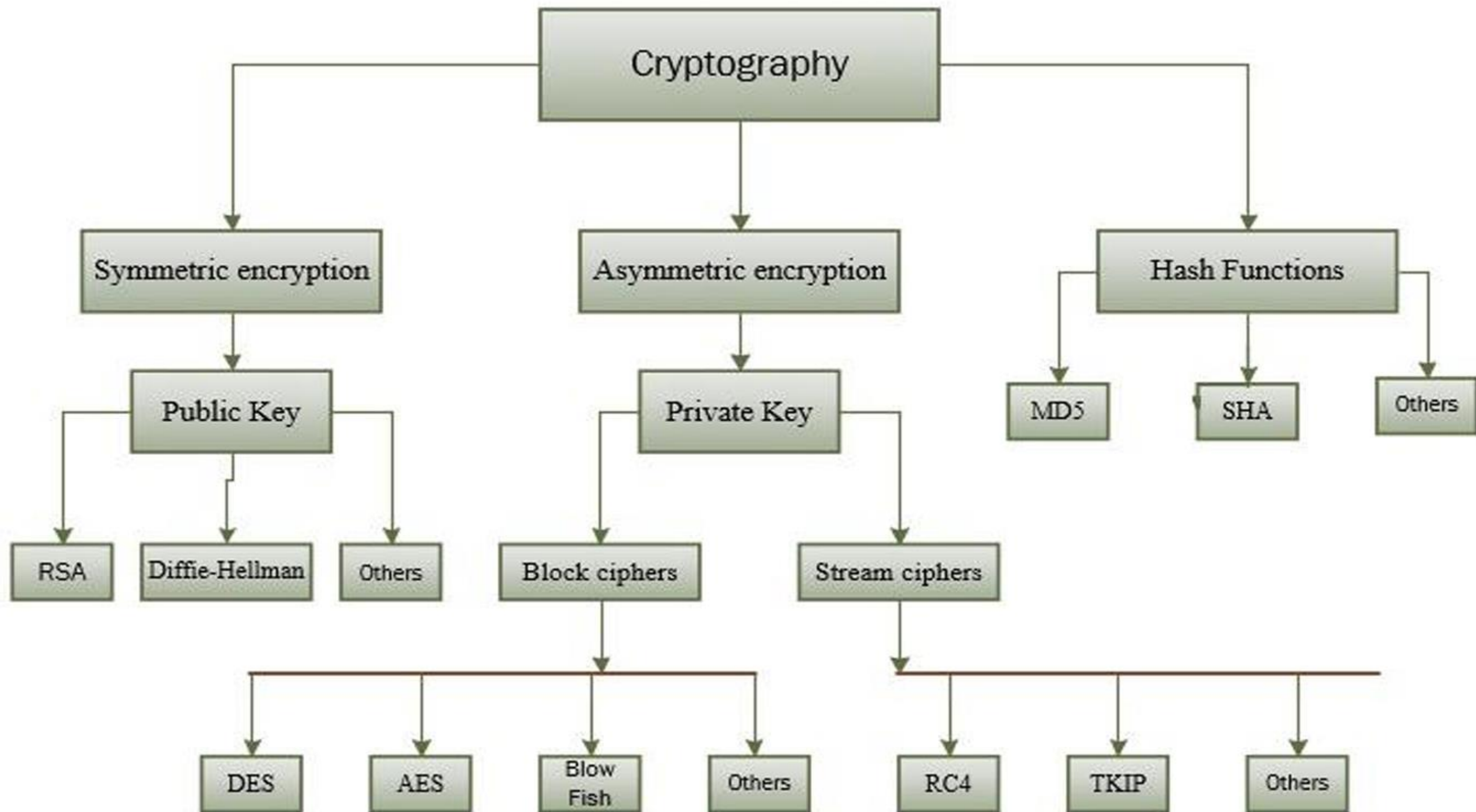
يستخدم نفس المفتاح للتشفير وفك  
يُستخدم في مهام مثل .التشفير  
تشفير الملفات.

2

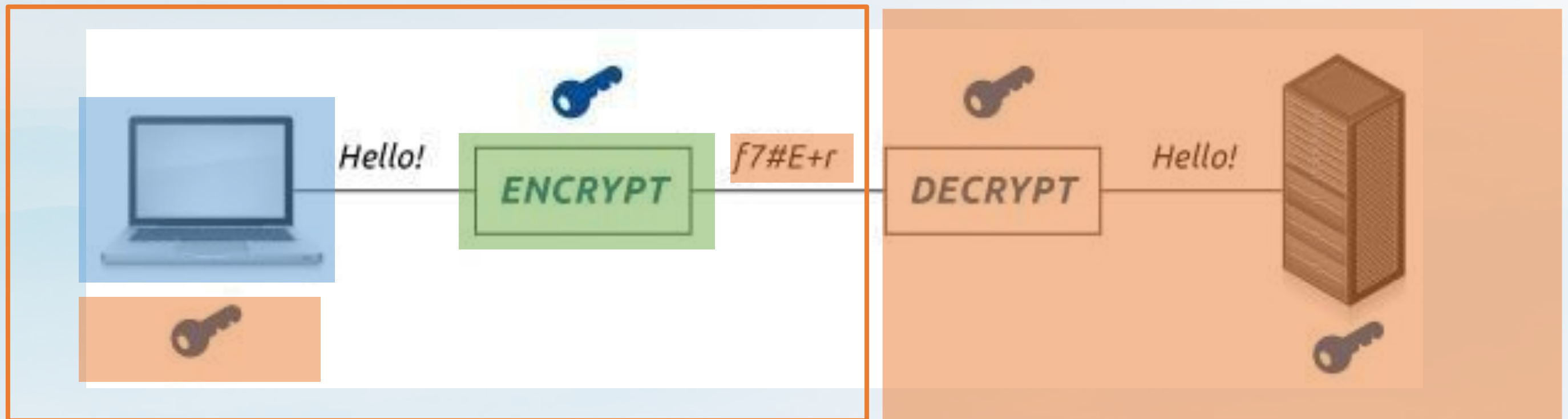
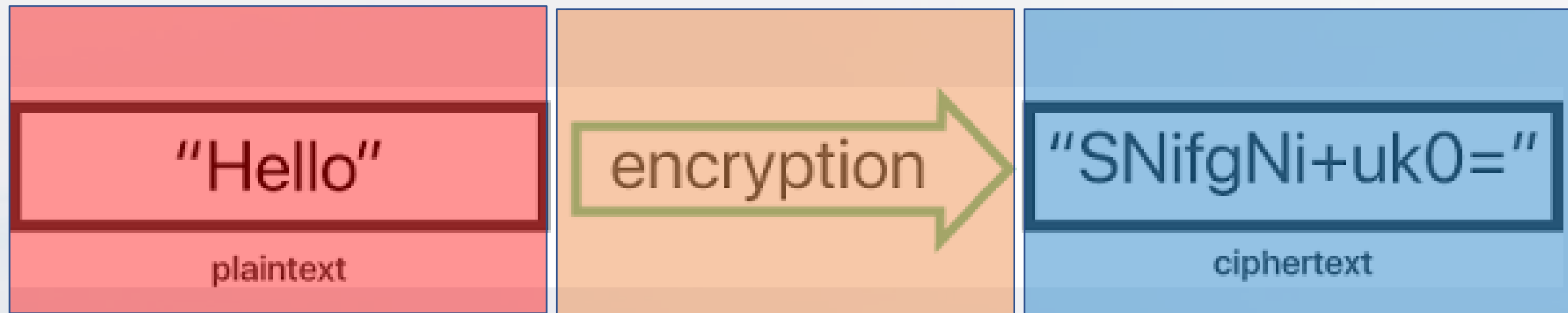
## التشفير غير المتماثل

مفتاح :يستخدم مفتاحين مختلفين  
عام للتشفير ومفتاح خاص لفك  
يُستخدم في مهام مثل .التشفير  
التوقيع الرقمي.









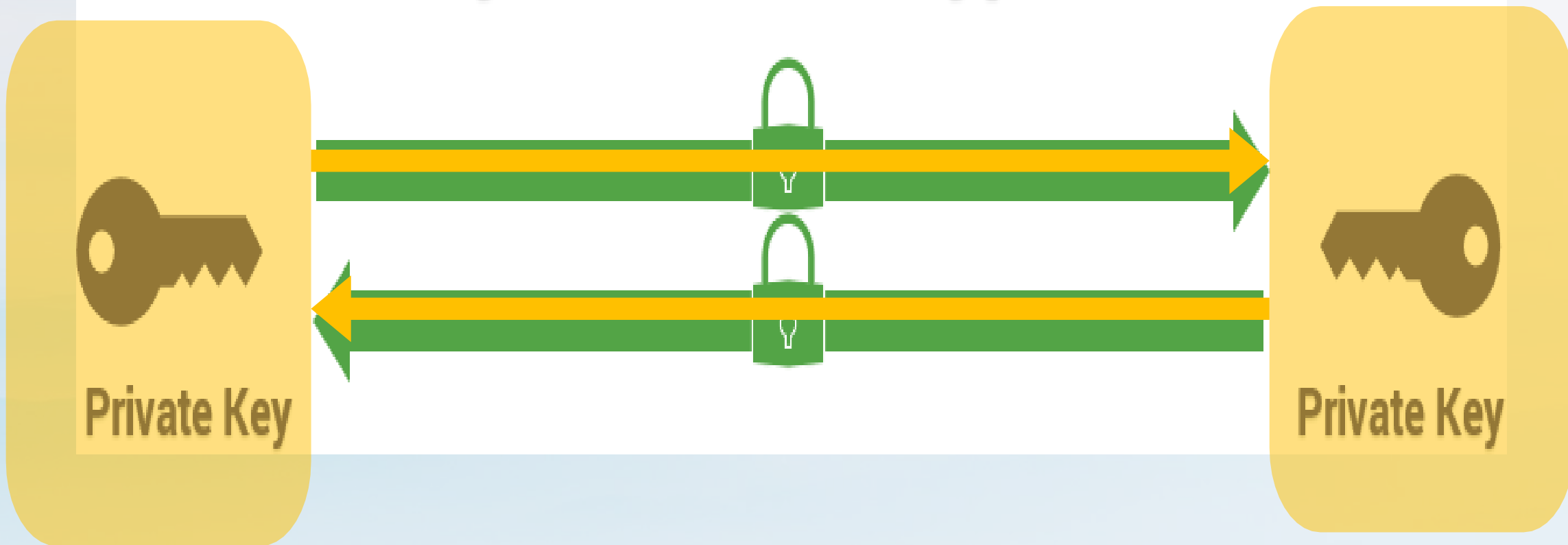
## Symmetric Encryption



## Asymmetric Encryption

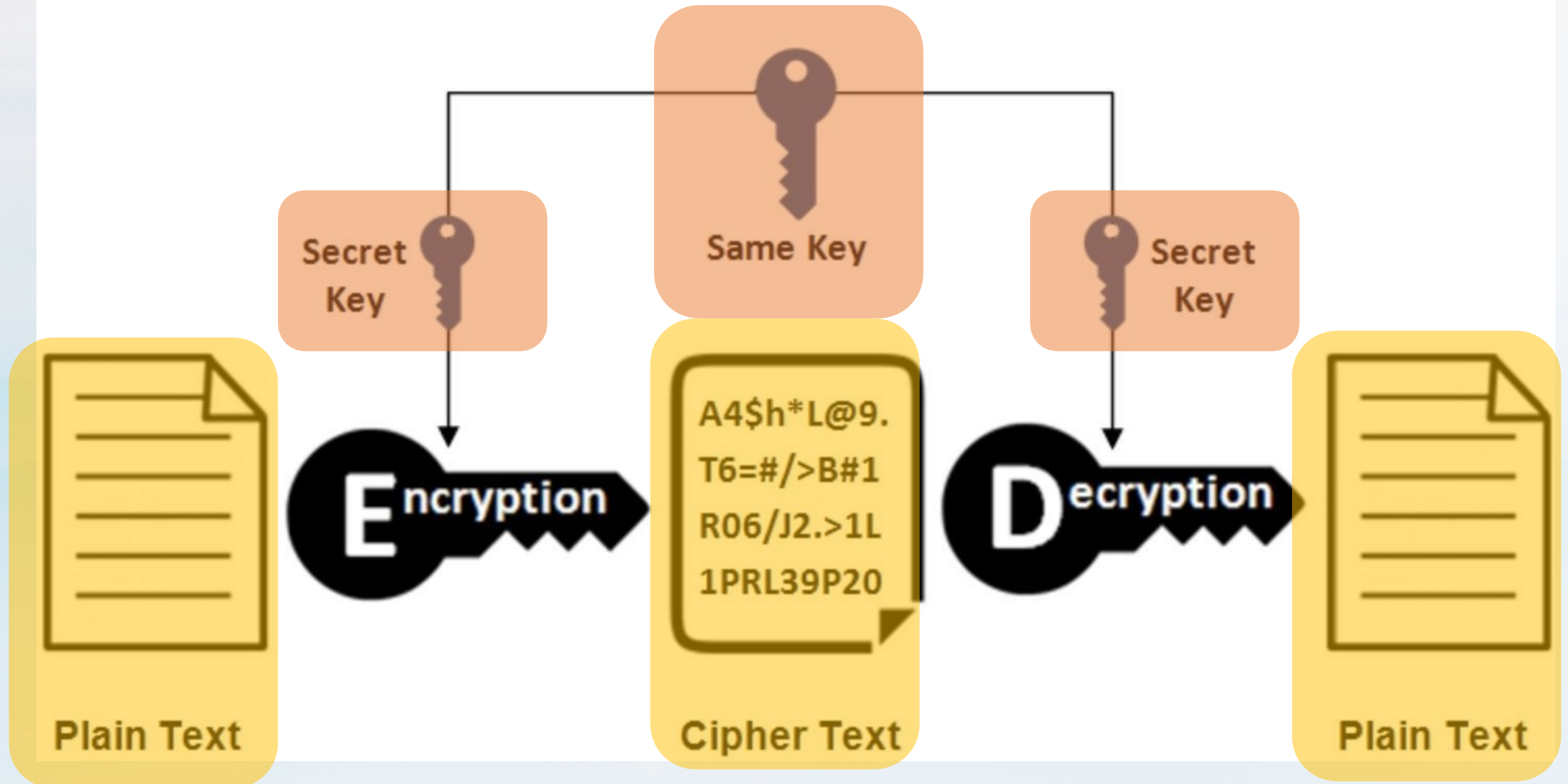


# Symmetric Encryption





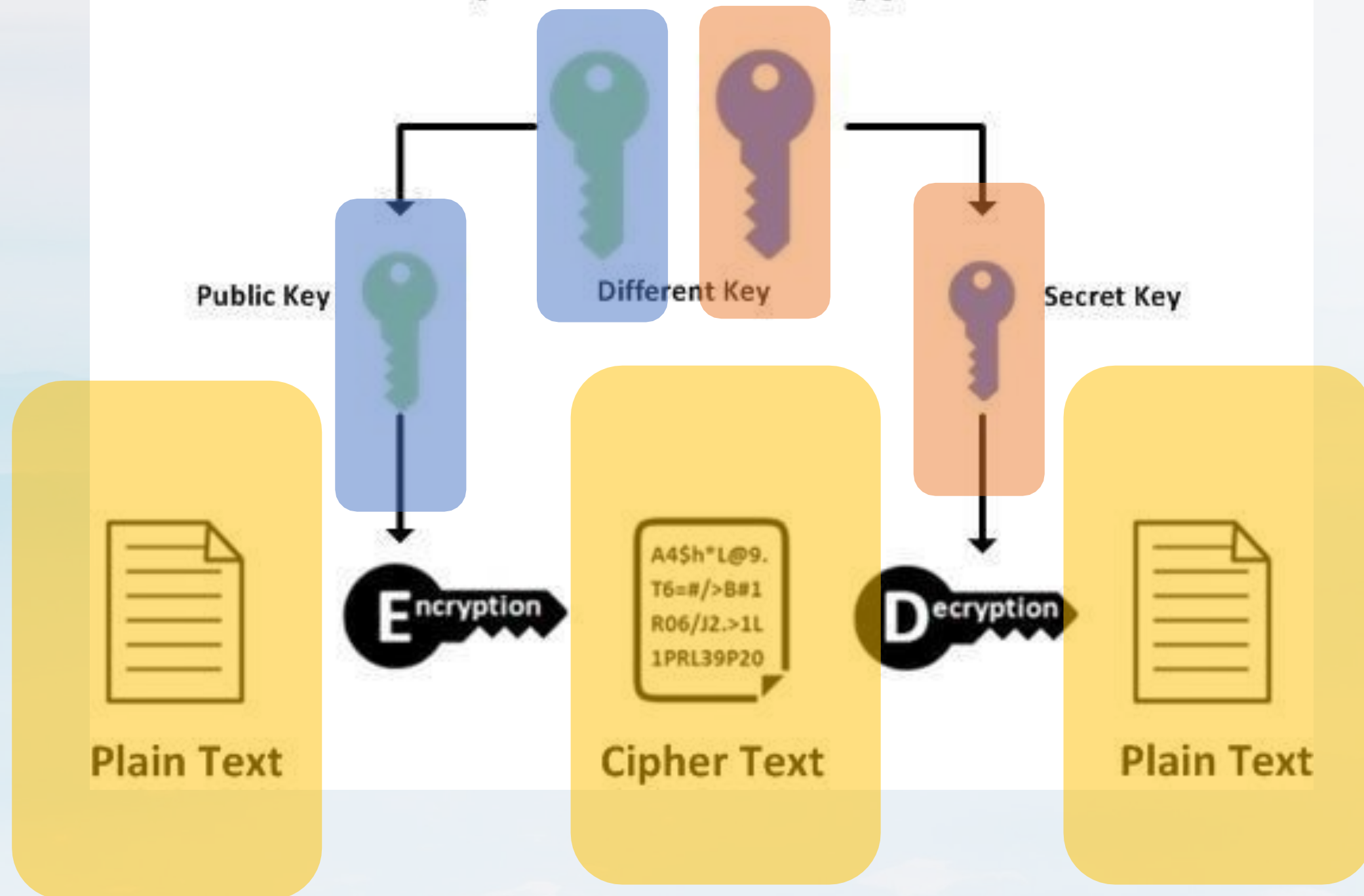
# Symmetric Encryption



# Asymmetric Encryption



# Asymmetric Encryption





# تحديات وأمن التشفير

1

## الاختراقات

حاولات غير قانونية لاختراق أنظمة التشفير للحصول على البيانات

2

## التطورات التكنولوجية

ظهور تقنيات جديدة قد تؤثر على فعالية خوارزميات التشفير

3

## الخصوصية الرقمية

توازن بين الحاجة إلى أمان البيانات والحفاظ على الخصوصية





# تقنيات التشفير العملية

1

اختيار خوارزمية التشفير  
المناسبة.

2

توليد مفاتيح التشفير

3

تشفير البيانات باستخدام

4

فك تشفير البيانات باستخدام  
المفتاح.

# تنفيذ التشفير في تطبيقات العالم الحقيقي

## البنوك

يتم استخدام التشفير لحماية البيانات المالية للعملاء أثناء المعاملات عبر الإنترنت.

## البريد الإلكتروني

يتم تشفير الرسائل الإلكترونية لمنع الوصول غير المصرح به.

## تطبيقات التواصل

يتم تشفير محادثات المستخدمين لحماية خصوصياتهم.




# التوقيع الرقمي وشهادات التشفير

التوقيع الرقمي يعمل على تأكيد هوية المُرسِل، وتوفير مصادقة للرسالة، بينما تُستخدم شهادات التشفير للتحقق من هوية الإِلِكترُونِيَّة.

التوقيع الرقمي 

.ضمان أمن الرسالة ومصدرها

شهادات التشفير 

.التأكد من هوية المواقع الإِلِكترُونِيَّة

SSL/TLS 

.بروتوكولات أمنية تستخدم شهادات التشفير

# الهجمات على الأنظمة التشفيرية

تستهدف الهجمات على الأنظمة التشفيرية كسر نظام التشفير والوصول إلى البيانات

1

## هجمات القوة الغاشمة

تجربة جميع الاحتمالات الممكنة لكسر الرمز السري

2

## الهجمات الإحصائية

تحليل أنماط التشفير للكشف عن الرمز السري

3

## هجمات القناة الجانبية

استخدام المعلومات التي تُكشف خارج قنوات الاتصال





# تطبيقات تشفير البيانات

تُستخدم أنظمة التشفير في مجموعة واسعة من التطبيقات، مثل البنوك، والتجارة الإلكترونية، والحكومات.



## أجهزة المحمول

تشفير بيانات المستخدمين وحماية الخصوصية.



## أجهزة الكمبيوتر

تشفير بيانات المستخدمين والملفات الحساسة.



## الخوادم

حماية بيانات الشبكات والخدمات المهمة.



**Dex2jar**

**Androguard**

**IDA**

**Valgrind**

# **Reverse Engineering Tools**

**Nudge4j**

**OllyDbg**



# HW

كيف احمي بياناتي الشخصية  
وفقكم الله

