其他内容可访问博客：either fight | or die (yst-10.github.io)

Cryptography and Cyber Security——Block1

一. 介绍

1.Internet Security

• A security system is typically introduced to: 一个安全系统通常涉及

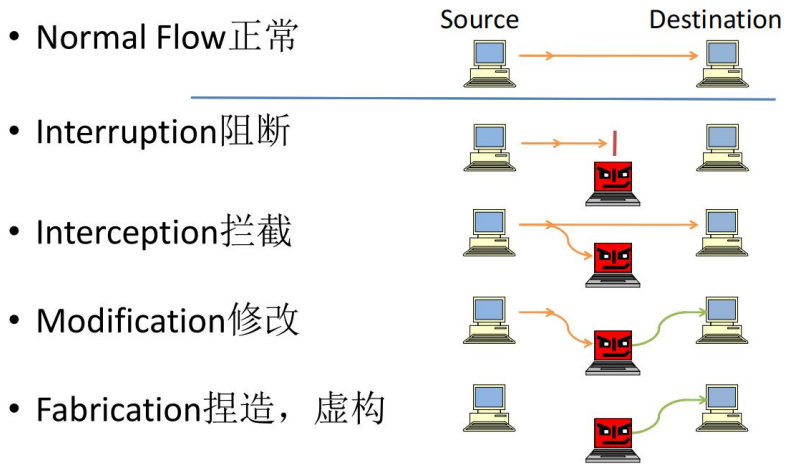
Deter(阻止), Prevent(防止), Detect(检测) and Correct(纠正) security violations of data transmission.对数据传输的安全违规行为。

2.Security Architecture(3 个)！！！

(1)Security Attacks

定义：Actions involving the compromise of security info.涉及安全信息泄露的行为。

Terminologies of Security Attacks!!!



<1>Passive Attacks(2 条)

①Release of message contents 消息内容泄露： Intercept info

②Traffic Analysis 流量分析： Analysis of traffic volume data

Traffic Analysis（流量分析）是一种计算机网络中的安全攻击，它通过监视和分析网络流量，以了解网络中正在进行的通信活动。攻击者可以使用流量分析来获取敏感信息、窃取凭据、获取通信内容、确定网络拓扑结构等。

常见的流量分析技术包括：

1. 被动监听：监视传输数据的过程，但不对数据进行任何修改或干扰，例如 Wireshark 等抓包工具。
2. 洪水攻击：向目标计算机发送大量的请求或数据包，从而使其网络不可用。洪水攻击也可以用于混淆流量、隐藏真正的攻击活动。
3. 端口扫描：尝试连接目标系统的每个端口，以确定哪些端口是打开的，并且可能存在漏洞或易受攻击。
4. DNS 污染：篡改 DNS 解析过程，使用户在访问某个网站时被重定向到伪造的网站，从而窃取用户的登录凭据或其他敏感信息。
5. SSL 中间人攻击：攻击者篡改 SSL/TLS 通信，欺骗双方认为他们正在直接通信，从而窃取敏感信息或执行其他恶意操作。

为了防止流量分析攻击，可以采用以下措施：

1. 加密通信：使用加密协议和技术，例如 SSL/TLS、SSH 等，保护数据的机密性和完整性，防止被窃听、篡改或伪造。
2. 使用 VPN：在公共网络上建立虚拟专用网络（VPN），加密通信并隐藏用户的真实 IP 地址，从而保护用户的隐私和安全。
3. 防火墙设置：配置网络防火墙来检测和拦截恶意流量，并限制对受保护系统的未经授权访问。
4. 流量混淆：使用技术，例如随机数据包生成、数据包大小调整等，以使流量更难分析和识别。
5. 检测工具：使用流量分析检测工具来监视网络流量，并及时发现异常活动和潜在的攻击威胁。

<2>Active Attacks (4 条)

①Masquerade: Capture and replay of valid authentication sequence 捕获和重播有效的身份验证序列

Masquerade（伪装）是一种网络攻击技术，攻击者通过伪装成合法用户、设备或系统的身份来获取未授权访问、窃取敏感信息或进行其他恶意活动。

1. IP 地址伪装：攻击者使用虚假的 IP 地址来隐藏自己的真实身份或欺骗目标系统，以获得未授权访问权限。
2. MAC 地址伪装：攻击者修改或伪造网络接口卡（NIC）的 MAC 地址，从而欺骗网络设备或系统，使其认为攻击者是合法用户或设备。
3. 电子邮件伪造：攻击者伪造电子邮件的发件人地址，使其看起来像是来自可信的发送者，以进行钓鱼、传播恶意软件或进行其他欺诈行为。
4. 网站伪装：攻击者创建虚假的网站，外观和功能与合法网站相似，诱使用户输入敏感信息或下载恶意内容。
5. 用户身份伪装：攻击者冒充合法用户的身份，并使用其凭据登录系统或访问受限资源。

为了防止伪装攻击，可以采取以下措施：

1. 强化身份验证：使用强密码、多因素身份验证（如指纹、智能卡、独立密码令牌等）来确保用户身份的真实性。
2. 加密通信：使用加密协议（如SSL/TLS）加密敏感数据的传输，防止被攻击者窃听或篡改。
3. 数字证书：使用数字证书来验证网站的真实性和完整性，防止被攻击者伪装为受信任的网站。
4. 防火墙和入侵检测系统：配置网络防火墙和入侵检测系统来检测和拦截伪装流量和恶意行为。
5. 安全教育和意识培训：提高用户对伪装攻击的认识，教育他们如何辨别和应对潜在的伪装威胁。

最重要的是，及时更新系统和软件，修补已知的漏洞，以减少攻击者利用已知漏洞进行伪装的可能性。

② Replay : Re-use of observed data to produce an unauthorised effect.重复使用观察到的数据，以产生未经授权的效果。

Replay（重放攻击）是一种网络安全攻击，攻击者通过记录和重播有效网络通信流量，来欺骗系统并获得未授权的访问或执行恶意操作。在重放攻击中，攻击者截获先前的网络通信，并将其重放到目标系统上，使目标系统误以为这是合法的通信。

重放攻击可以用于窃取敏感信息、绕过身份验证、伪造交易、欺骗系统等。以下是一些常见的防范措施：

1. 加密通信：使用加密协议（如SSL/TLS）来保护通信的机密性和完整性。加密可以防止攻击者截获通信流量并成功地进行重放攻击。
2. 时间戳和随机数：在通信中引入时间戳和随机数，以确保每个通信都是唯一的和不可预测的。这样可以防止攻击者重放先前的请求。
3. 消息认证码（MAC）：使用MAC来验证消息的完整性和真实性。在发送消息时，附加一个MAC，接收方可以使用相同的密钥验证消息是否被篡改。
4. 单次性令牌（One-Time Password，OTP）：使用OTP来生成一次性密码，确保每个请求都是唯一的。这可以有效防止重放攻击。
5. 防火墙规则：配置网络防火墙来检测和阻止异常的通信重放流量。例如，根据时间戳或其他特征，防火墙可以拦截重复的请求。
6. 会话管理：实施适当的会话管理机制，如使用会话令牌、定期重新验证身份等，以限制和防止重放攻击。
7. 安全加固：确保系统和应用程序是最新的，并修补已知的安全漏洞。同时，限制对敏感操作和资源的访问权限，减少重放攻击的潜在影响。

③*Modification of message contents* 修改信息内容 ：*Or part of it.*

修改消息内容是一种网络攻击行为，攻击者在传输过程中修改通信的内容，以达到其自己的目的。通过修改消息内容，攻击者可以进行各种恶意活动，例如篡改数据、欺骗用户、传播虚假信息等。

以下是一些防范修改消息内容攻击的常见方法：

1. 加密通信：使用加密协议（如SSL/TLS）来确保消息的机密性和完整性。加密可以防止攻击者窃听或篡改通信内容。
2. 数字签名：使用数字签名技术对消息进行签名，以验证消息的真实性和完整性。接收方可以使用相应的公钥来验证签名，并确保消息没有被篡改。
3. 哈希函数和消息验证码（HMAC）：在发送消息之前，使用哈希函数或HMAC生成一个摘要，并将其附加到消息中。接收方可以使用相同的哈希函数或密钥来验证摘要的一致性，以检测是否有人篡改了消息内容。
4. 安全协议：选择安全性较高的协议来传输消息，例如HTTPS，它结合了SSL/TLS加密和身份验证机制，能够有效地保护通信内容不被篡改。
5. 安全编码实践：在开发应用程序时采用安全编码实践，包括输入验证、防止跨站脚本（XSS）攻击和SQL注入等安全漏洞，以减少攻击者对消息内容的修改机会。
6. 消息完整性检查：接收方在接收到消息后，应进行完整性检查，验证消息的内容是否被篡改。如果发现任何异常或不一致，应中断通信并采取相应的措施。
7. 安全培训和意识提高：提高用户和开发人员对修改消息内容攻击的认识，教育他们识别和应对潜在的威胁。

④*Denial of Service: Inhibits the normal use of the network.* 禁止对网络的正常使用。*E.g. Network flooding or redirection of traffic.*

拒绝服务（*Denial of Service*，*DoS*）是一种网络攻击，旨在通过超载或破坏目标系统的资源，使其无法提供正常的服务给合法用户。攻击者通过利用目标系统的弱点或发送大量请求来消耗系统的计算能力、存储资源、带宽等，从而导致服务不可用。

(2)Security Mechanisms

定义：*Detection, prevention and recovery from attacks.*

- *There is no single mechanism to provide information security.*目前还没有提供信息安全的单一机制。
- *However, the element that underlies most of the security mechanisms is the use of 'Cryptographic Techniques'.*

然而，大多数安全机制的基本要素是“加密技术”的使用。

- ***Cryptography*** *is the art of secret writing, is the process of converting*

information, such as this slide, that can be read by most, into a secret code, that can only be read by those who are party to the secret.

密码学是一种秘密写作的艺术，是一种转换信息的过程，比如这张幻灯片，可以被读取成一个秘密代码，只能被参与秘密的一方读取。

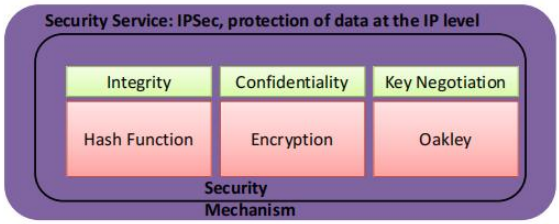
(3)Security Services

定义：*Processes which improves security and protects from attacks.*可提高安全性和保护用户免受攻击的过程。

- **Authentication** 身份认证 make sure not fake
  - Assurance of valid users and logical connections.
    保证有效的用户和逻辑连接
- **Access Control** 访问控制
  - Prevention of unauthorised used of recourses.
    防止未经授权使用的资源
- **Data Confidentiality** 数据保密性
  - Protection from unauthorised disclosures
    防止未经授权的信息披露
- **Data Integrity** 数据完整性
  - Assurance of valid/unchanged data.
    保证有效的/未改变的数据。
- **Non-repudiation**不被拒绝
  - Protection against denial from either party.
    防止被任何一方拒绝的保护措施。
- **Data Availability**数据可用性

例如：IPSec

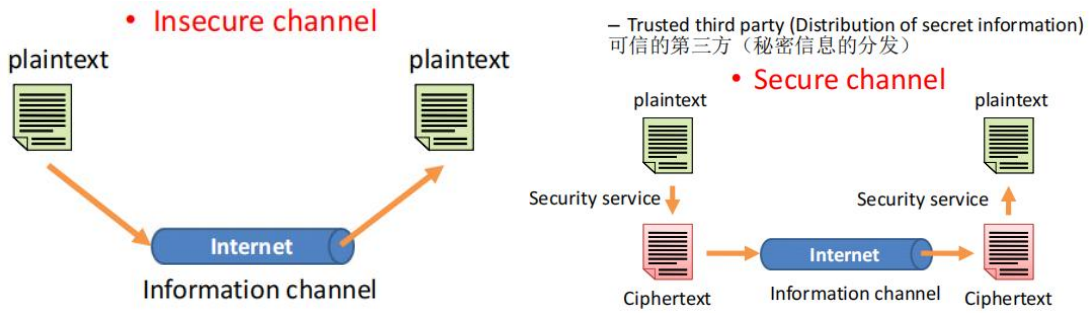
- One or more security mechanisms are combined to provide a security service.结合了一个或多个安全机制来提供一个安全服务。
  - IPSec, protection of the data at the IP level.
  - Ensures adequate security of the system resources and data transfer.



Terminology 总结

	Term	Description
Security	Plaintext	Original message
	Encryption	Encoding the message to hide its contents
	Ciphertext	Encrypted message
	Decryption	Retrieving the plaintext from ciphertext
	Key	Is used by the encryption and decryption. The decryption can be performed only by knowing the proper key.
Mechanism	Encryption	Confidentiality, authentication, integrity protection.
	Check/Hash algorithms	Integrity protection, authentication
	Digital signatures电子签名	Authentication, integrity protection, non-repudiation.
Services	Access control	Unauthorised user
	Confidentiality	Disclosure of unauthorised identities
	Integrity	Unauthorised data alterations
	Non-repudation	Originator of communications , later denying it
	Authentication	Assurance of someone's identity

3.A model of Internet security



注意：

• Security is assessed by the attacks, services and mechanisms

安全性通过攻击、服务和机制进行评估

• Several security mechanisms can be combined to provide a 'Security Service'.

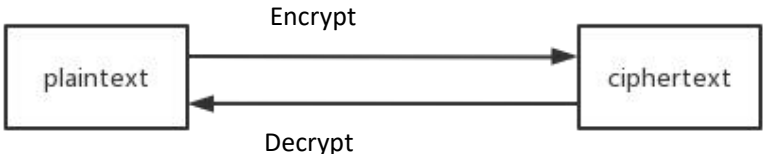
可以结合使用几种安全机制来提供一个"安全服务"。

• The main security mechanisms used in the internet are based on cryptographic techniques.在互联网中使用的主要安全机制是基于加密技术的

• The terminology in encryption is: plaintext, ciphertext, encryption, decryption and key. 加密技术中的术语是：明文、密文、加密、解密和密钥。

• Different security mechanisms protect against different attacks.

不同的安全机制可以防止不同的攻击。



二. Encryption 加密

1.Caesar Cipher

• *Caesar cipher, is a* ***stream cipher****, that uses simple* ***monoalphabetic substitution****.*

凯撒密码，是一种流密码，它使用简单的单元字母替换。

• **Key:** new letter = old letter +3

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

• **Example:**
Julius Caesar ➔ Mxolxv Fdhvdu

Mathematical expression of Caesar Cipher

• Assign a number to each letter, a=0, b=1, ... z=25

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Key= number of spaces forward in alphabet from plaintext letter
Note: **m** = plaintext, **k** = secret key, **c** = ciphertext

$c = m + k = m + 3$ or, more formally, $(m + 3) \bmod 26$

mod 26 refers to the modulo. Modulo is the operation of finding the Remainder when you divide two numbers. So, c cannot be > 26

E.g. letter J becomes letter M i.e. [9(letter J) + 3(Key)]mod26 = 12(letter M)

例题：

• Caesar wants to arrange a secret meeting with Marc Anthony, either at the Tiber (the river) or at the Coliseum (the arena).

• He send the ciphertext **EVIRE**.
密码：13,4 两个都行

2.Vigenère Cipher

• *There are stream ciphers that use* ***poly-alphabetic*** *substitution.* 多字母替换

- **Plaintext**: my password is tomato
- **Key**: stream

PlainText	M	Y	P	A	S	S	W	O	R	D	I	S	T	O	M	A	T	O
Key	S	T	R	E	A	M	S	T	R	E	A	M	S	T	R	E	A	M
Ciphertext	E	R	G	E	S	E	O	H	I	H	I	E	I	H	D	E	T	A

- Using numbers:
  - M → 12 plaintext
  - S → 18 key

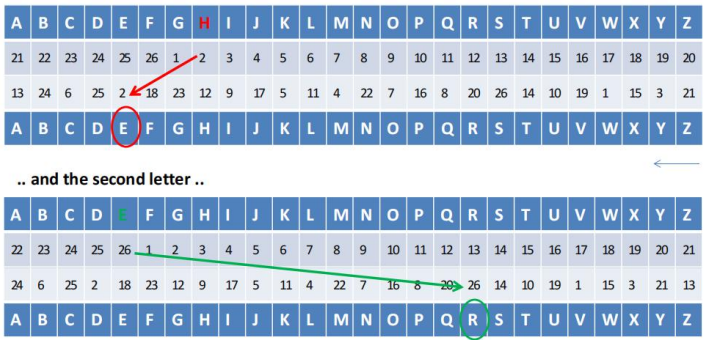
- Encryption:
  - (12+18)mod26 = (30)mod26 = 26 + 4 = 4
  - 4 → E Ciphertext

暗文=（明文＋key）与 26 取余

3.Rotor Encryption

HELLO → EROFW

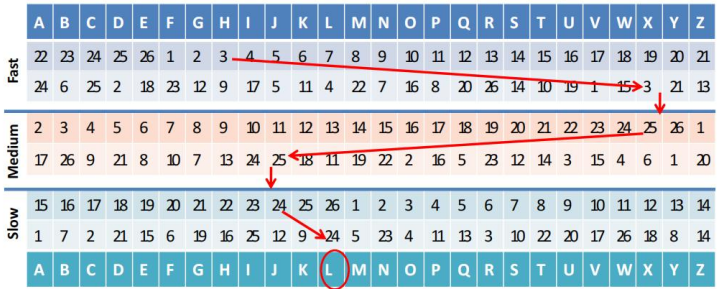
26 Alphabets



解析：
1.先是明文第一个字母 H 对应数字 2，2 对应 E，找到暗文第一个字母 E 结束；
2.两排数字同时向左移动；
3.明文第二个字母 E 对 26,26 对应 R，找到暗文第二个字母 R；
4.重复以上

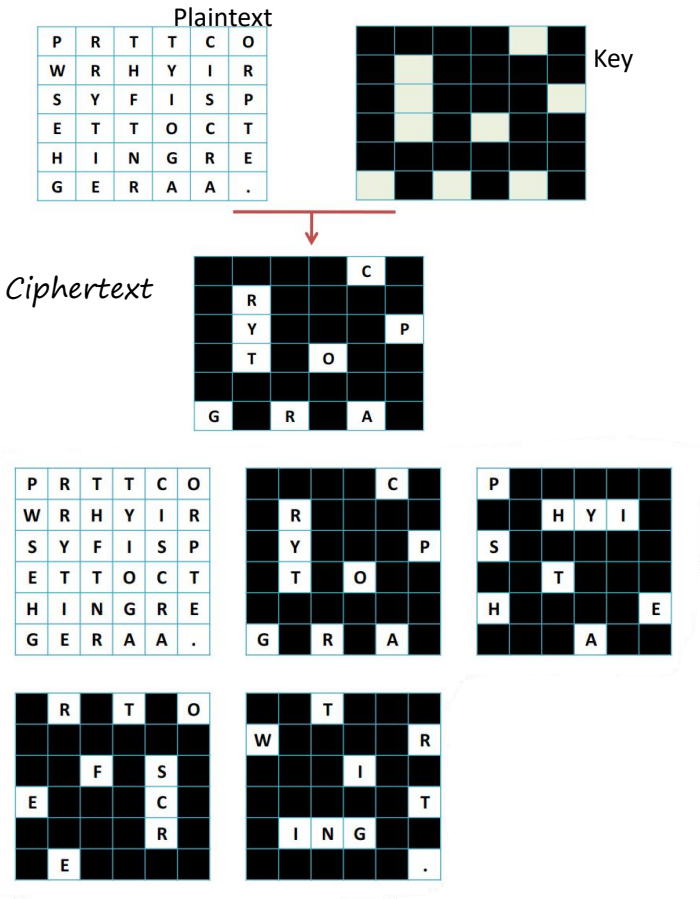
If 3 rotors → 26^3 = 11,567
If 5 rotors → 26^5 = 11,881,376 Alphabets

- HELLO → L....



注意左侧，多拐几个弯

4.Transposition: The Grille



解析：

（1）把 Key 放在明文上面得到第一组单词（一排一排读）；

（2）顺时针旋转 90 度得到第二组单词；

（3）继续顺时针旋转 90 度，一共四次。

Ciphertext:
cryptography is the art of secret writing.

三. Classification of Cryptographic Systems 分类

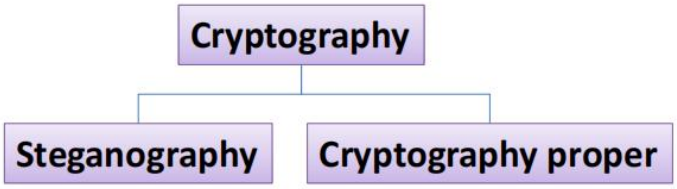
1.Classification of Steganography & Cryptographic Methods

- **Steganography (covert secret writing) 隐写术**

– covert writing, is where it is not evident that there is a secret message 秘密写作，是指不明显存在秘密信息

- **Cryptograph proper (overt secret writing) 公开**

– Overt writing, is evident that there is a secret message.公开写作，很明显有一个秘密信息。



2.Classification of Cryptographic Systems！！！

(1). The type of operations used for transforming plaintext to Ciphertext 用于将明文转换为密文的操作类型

• **Substitution**: Each element of the plaintext is mapped into another element.

(element = bit, letter, group of letters ...)

明文中的每个元素都被映射到另一个元素中。（元素=位，字母，字母组...）

• **Transposition**: Each element of plaintext is rearranged.

明文中的每个元素都被重新排列。

Method	Example	Explained..
Substitution	Caesar ➔ Mxolxv	Substitute one letter for another.
Transposition	Caesar ➔ raaCse	Change the order of the letters.

Diffusion and Confusion (Shannon):

No information is lost, and the operations are reversible.

(2). The number of keys used

- **Symmetric:** Sender and receiver use the same key.
  - This is known as '***conventional encryption***'.

Also known as 'Single-key' & 'Secret-key'

- **Asymmetric:** Sender and receiver each use a different key.
  - This is known as '*public-key encryption*'.

Also known as 'Two-key' encryption.

(3). The way in which the plaintext is processed

• **Stream Cipher**: Process one input element at a time.

流密码：一次处理一个输入元素。

• **Block Cipher**: Process a block of elements at a time.

块密码：一次处理一个元素块。

3.Stream Ciphers

- **Notation:**
  - **m** = plaintext, **k** = secret key, **c** = ciphertext
  - **e** = encryption function, **d** = decryption function
- **Encryption:**
  - $c = e_k(m)$
  - $c_i = m_i \oplus s_i$
  - Where: i = 0,1,...., s_i = key bit stream, and $\oplus$ is the XOR function
- **Decryption:**
  - $m = d_k(c)$
  - $m_i = c_i \oplus s_i$
  - **Example**

ASCII	
A	01000001
B	01000010
C	01000011
D	01000100
:	:

XOR

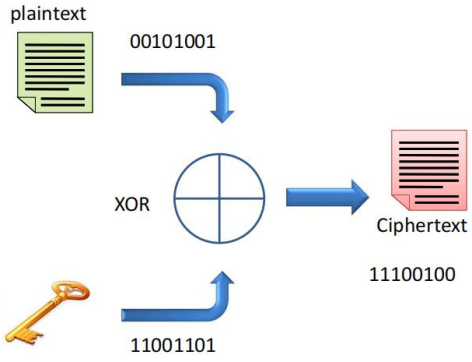
Input	Output
$0 \oplus 0$	0
$0 \oplus 1$	1
$1 \oplus 0$	1
$1 \oplus 1$	0

plaintext	1	0	1	1	0	1	1	1	0	..
key	0	0	1	1	1	0	1	0	1	..
ciphertext	1	0	0	0	1	1	0	1	1	..

- *Notice that the composition of two XOR's is identical to the original data.*

Input	Output
$0 \oplus 0$	0
$0 \oplus 1$	1
$1 \oplus 0$	1
$1 \oplus 1$	0

请注意，两个 XOR 的组成与原始数据相同。



注意：

- **Encryption can be very fast 加密的速度可以非常快**
- **No error propagation, but .. 无错误传播，但是**

– No protection against message manipulation 没有针对消息操作的保护功能

– It is easy to determine the key-stream if one knows the plaintext and ciphertext

如果人们知道明文和密文，就很容易确定 key

– If one bit, in either the message or key, is in error then the entire piece of cypher text will become corrupted 如果消息或 key 中的一位是错误的，那么整个密码文本将被损坏

4.One Time Pad

(1)There is a stream cipher that is unbreakable, 一种牢不可破的流密码，

(2)How it works?

– For each message use a new random key that is as long as the message.

对于每条消息，请使用一个新的随机密钥，其长度与该消息一样长

– Encryption output that has no statistical relationship to the plaintext. 与明文没有统计学关系的加密输出

(3)**Applications** – Secure media

(4)**Vulnerabilities** 弱点

– The practical difficulty is how to transmit and protect the random key. 实际上的困难在于如何传输和保护随机密钥。

– Message manipulation 消息操作

– Like other stream ciphers, easy to get wrong!像其他流密码一样，易出错

- The following messages and keys produce the same ciphertext

M	R	M	U	S	T	A	R	D	W	I	T	H	T	H	E	C	A	N	D	L	E	S	T	I	C	K	I	N	T	H	E	H	A	L	L
P	X	K	M	V	M	S	Y	D	O	E	U	Y	R	V	Y	W	C	S	N	L	E	B	N	E	C	V	G	D	U	O	A	H	E	N	B
M	I	S	S	S	C	A	R	L	E	T	W	I	T	H	T	H	E	K	N	I	F	E	I	N	T	H	E	L	I	B	R	A	R	Y	A
P	G	E	O	V	D	S	Y	V	G	T	R	X	R	V	J	R	Y	V	D	O	D	P	Y	Z	L	Y	K	F	F	U	N	O	N	A	M

B	O	W	G	N	F	S	P	G	K	M	N	F	K	C	C	Y	C	F	Q	W	I	T	G	M	E	F	O	Q	N	V	E	O	E	Y	M

- If you only know the ciphertiext which one is the original text?

注意：Encryption 使用 Vigenère cipher，The key length is equal to the plaintext length.

两组：每一组上面是 plaintext，下面是 key，绿色是 ciphertext

5.Simple Block Cipher

- Takes the letters and changes their order.
- **For example:**
  - Block size is 10 letters
  - Permutation: from {1,2,3,4,5,6,7,8,9,10} to {3,1,2,10,7,5,4,8,6,9}

Plaintext	Ciphertext
cryptography-is-the-art-of-secret-coding	ycrpgtproa-hy-tsih-etarc-o-sfetregdc-ion

plaintext	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	...
	C	R	Y	P	T	O	G	R	A	P	H	Y	-	I	S	-	T	H	E	-	
ciphertext	3	1	2	10	7	5	4	8	6	9	3	1	2	10	7	5	4	8	6	9	
	Y	C	R	P	G	T	P	R	O	A	-	H	Y	-	T	S	I	H	-	E	

6.Playfair square

(1).Uses a 5X5 table

– Contains a key word or phrase (without repeating letters) 包含一个关键字或短语（不带重复的字母）

– Then filled with the remaining alphabets. 然后填上剩下的字母表

– In order to fit the square, some systems omit the 'Q', and others combine the I&J in the same square 为了适合正方形，一些系统省略了"Q"，而另一些系统将 I&J 组合在同一正方形中

- Eg. "MY SECRET CODE IS" ➔MYSECRTODI

Key->

M	Y	S	E	C
R	T	O	D	I
A	B	F	G	H
K	L	N	P	Q
U	V	W	X	Z

(2).Break the message into groups of two letters and map them into the key table. The two letters of digraph are considered as opposite corners of a rectangle.

将消息分成两个字母的组，并将它们映射到关键表中。有向图的两个字母被认为是一个矩形的相对角。

<1>If the group consist of similar letters, insert a 'Q' or 'X'.

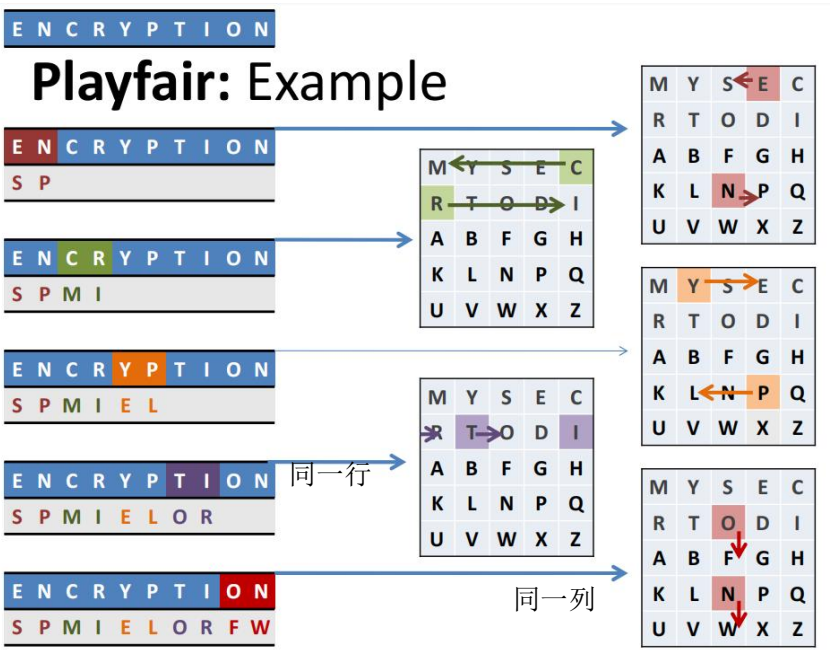
如果字母相同，插入 Q 或者 X

<2>If both letters are on the same row, replace them with their immediate right respectively (wrapping around)在同一行，都向右移动一步

<3>If both letters are on the same column, replace them with the letters immediately below (wrapping around) 在同一列，都向下移动一步

<4>All other letters must be replaced by the other two corners of the formed rectangle (in the order they are placed). 其他的替换为矩形的另外两个角（横着动）

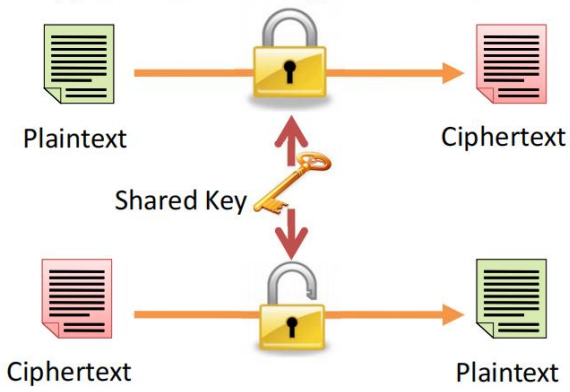
(3) *Decryption is achieved by inverting the process, with dropping any extra 'X' or 'Q' that don't make sense!* 解密是通过反转这个过程来实现的，即删除任何额外的没有意义的"X"或"Q"！



7.Security of conventional encryption 常规加密的安全性

- *Strong encryption algorithm* 强加密算法
- *Sender and receiver obtained the secret key in a secure fashion* 发送方和接收方以一种安全的方式获得了密钥
- *The key must be kept secure at all times* 钥匙必须始终保持安全

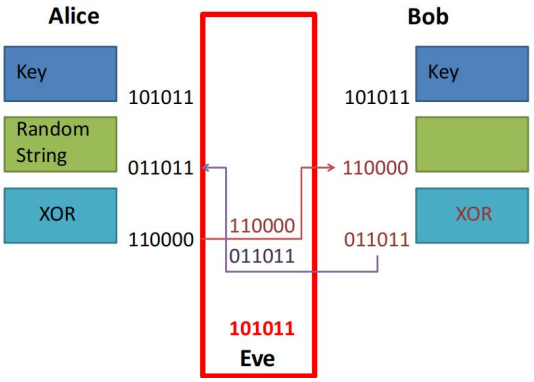
- Encryption and decryption share the same key



8.Key Agreements！！！

- In modern encryption the algorithms are public, the strength of the structure communication mechanism is based on the secrecy of the key.
  在现代加密技术中，算法是公开的，结构通信机制的强度是基于密钥的保密性。
- Hence key agreement is a security mechanism that is of fundamental importance as it deals with agreement on shared secure channel to exchange conventional encryption key因此，密钥协议是一种具有重要意义的安全机制，因为它处理共享安全通道交换传统加密密钥的协议
- To exchange the keys used for encryption we need:
  - Agreement of shared key共享密钥的协议
  - Secure channel to exchange conventional key通过安全通道交换常规密钥

例子：是否安全？



Alice 选择一个随机的比特串作为初始随机比特串，并将其与 key 进行 XOR 操作，得到结果 A。Alice 将结果 A 发送给 Bob。Bob 接收到结果 A 后，将其与自己的 Key 进行 XOR 操作，得到结果 B，并将结果 B 发送回 Alice。Alice 接收到结果 B 后，会检查它是否与她选择的初始随机比特串相匹配。如果匹配，则认为 Bob 拥有相同的秘密密钥。

Ans:???

四.Typical Attack Approaches and Cryptanalysis

- **Cryptanalysis Attacks: 密码分析攻击**

– The attacker relies on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintextciphertext pairs. 攻击者依赖于算法的性质，以及一些关于明文的一般特征的知识，甚至是一些样本明文密文对。

– The aim is to deduce a specific plaintext or the key being used. 其目的是推断出一个特定的明文或被使用的 key。

- **Brute-force Attacks: 蛮力攻击**

– The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. 攻击者尝试一段密文上的每一个可能的密钥，直到获得可理解的明文翻译。

– On average, the attacker succeeds after 50% of the trials.平均而言，攻击者在经过 50%的试验后都会成功。

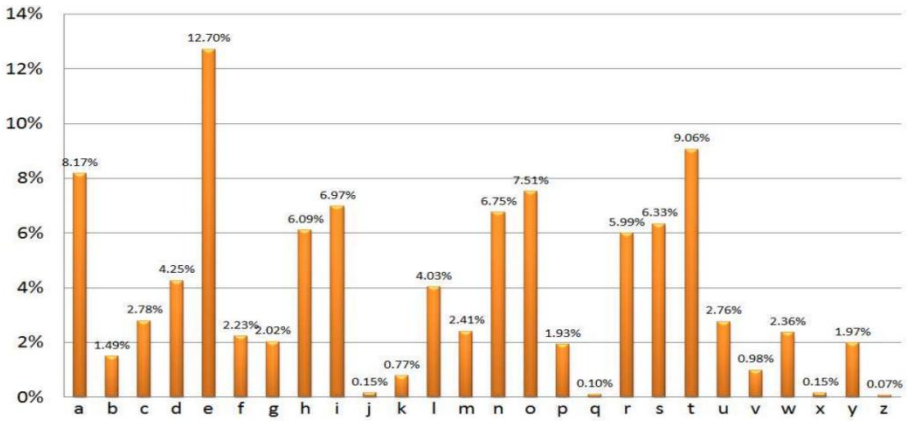
1.Cryptanalysis 密码分析

- **The process of attempting to discover the plaintext or key from the ciphertext.**试图从密文中发现明文或Key的过程。

- **In general, an encryption algorithm, is designed to withstand an attack even when**一般来说，加密算法被设计用来抵御攻击
  - The ciphertext密文
  - The encryption algorithm加密算法
  - One or more plaintext-ciphertext pairs formed with a secret key are known由一个密钥组成的一个或多个明文-密文对是已知的
- **This is known as a known-plaintext attack.**这被称为一种已知的明文攻击。

- **An encryption algorithm is computationally safe if ..**一种加密算法在计算上是安全的
  - Cost of breaking the cipher is much greater than the value of the encrypted information 破解密码的成本远远高于加密信息的价值
  - Time to break the cipher is much longer than the useful lifetime of the encrypted information 破解密码的时间比加密信息的有效寿命要长得多

Frequency Analysis 破解简单代码，利用语言规律!!!



2.Back to Caesar

Example：

(1)Original text

This is an example of how to test Caesar's method. After we take this example, we remove all punctuations and spaces from the original text. The outcome from this process is the 'plaintext' we require.

从原始文档中删除标点和空格，得到明文！！！

(2)Plaintext

thisisanexampleofhowtotestcaesarsmethodafterwetaket
hisexampleweremoveallpunctuationsandspacesfromth
eoriginaltexttheoutcomefromthisprocessistheplaintext
werequire

Key='f'

T	H	I	S	I	S	...
19	7	8	18	8	18	...
24	12	13	23	13	23	...
Y	M	N	X	N	X	...

+5 与 26 取模得到

(3)Ciphertext

YMNXNXFSJCFRUQJTKMTBYTYJXYHFJXFWXRJYMTIFKYJWBJYFPJ
YMNXJCFRUQJBJWJRTAJFQQUZSHYZFYNTSXFSIXUFHJXKWTRY
MJTWNLNSFQYJCYYMJTZYHTRJKWTRYMNXUWTHJXXNXYMJU
QFNSYJCYBJWJVZNWJ

(4) Frequency Analysis

A	B	C	D	E	F	G	H	I
1	4	4	0	0	13	0	5	2
J	K	L	M	N	O	P	Q	R
24	4	1	8	10	0	1	6	7
S	T	U	V	W	X	Y	Z	
6	12	6	1	9	13	19	4	

计算密文中字母出现的次数

计算字母出现次数/总次数

Our example

A	B	C	D	E	F	G	H	I
0.006	0.025	0.025	0.000	0.000	0.081	0.000	0.031	0.012
J	K	L	M	N	O	P	Q	R
0.149	0.025	0.006	0.050	0.062	0.000	0.006	0.037	0.044
S	T	U	V	W	X	Y	Z	
0.037	0.075	0.000	0.006	0.056	0.081	0.118	0.025	

下面为英语语言频率规律

English text frequency

A	B	C	D	E	F	G	H	I
0.082	0.015	0.028	0.043	0.127	0.022	0.020	0.061	0.070
J	K	L	M	N	O	P	Q	R
0.002	0.008	0.040	0.024	0.067	0.075	0.019	0.001	0.060
S	T	U	V	W	X	Y	Z	
0.063	0.091	0.028	0.010	0.024	0.002	0.020	0.001	

(5) Using vectors to find the key

- Write English text frequencies as a vector将英文语言的频率写成一个向量（固定）

$$\overline{A}_0 = (0.082, 0.015, 0.028, 0.043, \ldots, 0.001)$$

If $\overline{A}_0 = (f_0, f_1, f_2, \ldots, f_{25})$

and $\overline{A}_j = (f_j, f_{j+1}, \ldots f_{25}, f_0, \ldots, f_{j-1})$

Where $\overline{A}_j$ represents $\overline{A}_0$ shifted by *j* spaces to the right

Then the dot product is:

$$\overline{A}_i \cdot \overline{A}_j = f_i f_j + f_{i+1} f_{j+1} + f_{i+2} f_{j+2} + \ldots$$

- Examples:

$$\overline{A}_0 \cdot \overline{A}_0 = (0.082)^2 + (0.015)^2 + (0.028)^2 + \ldots + (0.001)^2 = 0.066$$

$$\overline{A}_0 \cdot \overline{A}_1 = 0.082 \times 0.015 + 0.015 \times 0.028 + \ldots + 0.001 = 0.039$$

76

Properties（固定）→

暗文的频率↓

*** Write the ciphertext frequencies as a vector**

$$\overline{W} = (0.006, 0.025, 0.025, 0.000, \ldots)$$

*** Evaluate** $\overline{W} \cdot A_0, \overline{W} \cdot A_1, \overline{W} \cdot A_2, \overline{W} \cdot A_3, \ldots, \overline{W} \cdot A_{25}$

|i - j|	0	1	2	3	4	5	...
$W.A_j$	0.028	0.04	0.035	0.029	0.036	0.066	...

77

←计算出 Key（上面的是性质固定计算与 key 无关）j=1，|i-j|=1，Aj 求法见上

3.Breaking the Vigenère cipher（求明文）

Example：

FHYULCVBYEBYJEUDSYQEAFELWRGFGCQI
SVBCVTIQOUQFMUDCYEJRPGQGRKEZOUCS
RGQTDRRRKEKRDCUNARMNXTCUHCZAQWHC
VOLRFZHNHDMGQBYEBYJEYZEYOTFBLMQD
MQBYQKCUHCDPNOICGHGVGCQISVTMPALB
PPRBJHMQKIQLNTHNRLOLVILFLSGERKEQ
SECGOKHTCUALGTFHCMZCYWCFHRRKEJHT
RHRGVEJHTRHRCHECH

The repetitions are multiples of 3. So take every third letter and make frequency analysis.

FHYULCVBY EBYJEU...重复次数是 3 的倍数，所以每次取第三个字母进行频率分析

(1)Length of key

←Plaintext table（只展示出部分）

<1>Copy and shift the ciphertext by one 复制并移动 1

<2>移动 2→

<3>移动 3，重复操作↑

得出总表→

Displacement	1	2	3	4	5	6	7	8	9	10
Coincidences	4	12	25	8	6	25	8	8	27	5

结果：If the displacement is a multiple of three we have a large number of coincidences,most probably the key is of size 3 如果位移是 3 的倍数，我们有大量的巧合，很可能 key 的大小是 3

(2)finding the key

因为 key 大小是 3，所以把 Plaintext 分为三组，第一组是第 1,4,7...字母，第二组是 2,5,8...字母，第三组是 3,6,9...字母。然后对每组字母进行频率分析

- **If the key is of size n then**
  - For *i*=1 .. n
    1. Compute the frequencies of the letters in positions *i* mod *n* and make the vector ***W*** 计算i组的字母频率，作为向量W
    2. For j = 0 ... 25 compute p_j = ***W.A***$_j$ W和Aj相乘得到p（i-j)的概率
    3. Let $k_i = j$ where p_j is the maximum value p最大时得到当时的j
  - The key is probably $\{k_1,k_2,\ldots,k_n\}$

- **Our example**
  - Key = {3,0,24} = DAY

破解得到明文！！！注意：要满足字母规律，补 E

CHARLESBABBAGEWASANECCENTRICGEN CHARLES BABBAGE WAS AN ECCENTRIC GEN
IUSBESTKNOWNFORDEVELOPINGTHEBLU IUS BEST KNOWN FOR DEVELOPING THE BLU
EPRINTFORTHEMODERNCOMPUTERHEWAS EPRINT FOR THE MODERN COMPUTER HE WAS
THESONOFBENJAMINBABBAGEAWEALTHY THE SON OF BENJAMIN BABBAGE A WEALTHY
LONDONBANKERHEAPPLIEDHISGENIUST LONDON BANKER HE APPLIED HIS GENIUS T
OMANYPROBLEMSHISINVENTIONSINCLU O MANY PROBLEMS HIS INVENTIONS INCLU
DETHESPEEDOMETERANDTHECOWCATCHE DE THE SPEEDOMETER AND THE COW CATCHE
RTHELETTERISELETTEREEEEE R THE LETTER IS E LETTER EEEEE

（3）总结分析（上面 1,2）

1. Determine the key length of the keyword (m)

- **Kasiski test**:
  - Search ciphertext for pairs of identical segments 搜索相同的密文段对（如之前的BY）

- **Index of coincidence**:符合指数
  - Suppose $x=x_1,x_2,\ldots,x_n$ is a string of length n. The index of coincidence of x is defined as the probability that two random elements of x are identical.假设x=x1， x2， ...， xn是一个长度为n的字符串。x的符合指数定义为x的两个随机元素相同的概率

2. Determine each of the keys (K_i) separately; hence, $K=(K_1,K_2,..,K_m)$

五. Applications(encryption codes)

Technology	Comments
WEP 128Bit	Wired Equivalent Privacy, the security system built into 802.11b wireless LAN equipment. Its RC4 basses encryption was broken by AT&T Engineers.
CMEA 64bit	Cellular Message Encryption Algorithm, this is supposed to ensure privacy on digital cell phones.
DES 56bit	Digital Encryption Standard, used throughout the Internet and other systems.
PGP 56bit	Pretty Good Privacy, a popular e-mail and file security program.
S/MIME 40bit	An RSA based encryption system to earlier versions of secure Outlook Express, and some other e-mail systems
CLSID Microsoft MSN and e-mail security. Microsoft SSH 40bit	SSH is a widely used client-server application for authentication and encryption of network communications.
QNX	Stock Exchange's facility security system, and VISA International's transaction processing and verification system.
RSA RC5 56bit	RC5 Is one of the more common implementations by RSA. It is used widely throughout business and the Internet.
SDMI	Secure Digital Music Initiative is the digital watermarking system designed to prevent MP3's from being copied.
RC4/MD5 128bit	This is the security used in all of Microsoft's "Office" products for password security, core design by RSA.
SSL/RC4 128bit	The Secure Socket Layer or SSL is based on RSA's RC4 and has been hacked in its "strong" form. This is the "secure" in virtually every online credit card ordering system and secure web page.
GSM Phones	The algorithm that secures more that GSM digital phones worldwide.

六. Conventional Encryption and DES

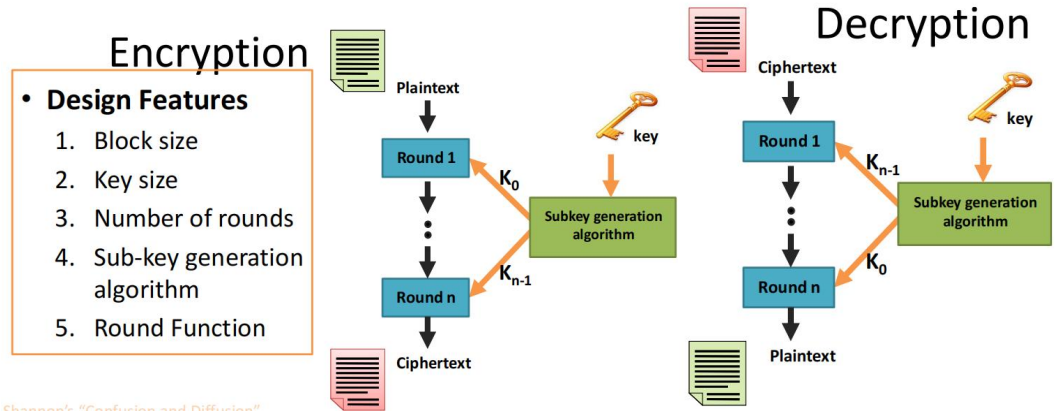
1.Block Ciphers

• A block cipher process one block of elements of the plaintext at a time. 一个块密码一次处理明文中的一个元素块。

• It produces one block of ciphertext of same size as the plaintext.它产生一个与明文大小相同的密文块。

常规加密定义：Block ciphers that use a shared key (symmetric) are known as **conventional encryption** algorithms.使用共享密钥（对称）的块密码被称为传统的加密算法。

2.Feistel Algorithm



3.Data Encryption Standard – DES 数据保密标准

(1)概述

定义：Is a block cipher with:

- **Block size** : 64 bits
- **Key size** : 56 bits
- **Number of rounds**: 16

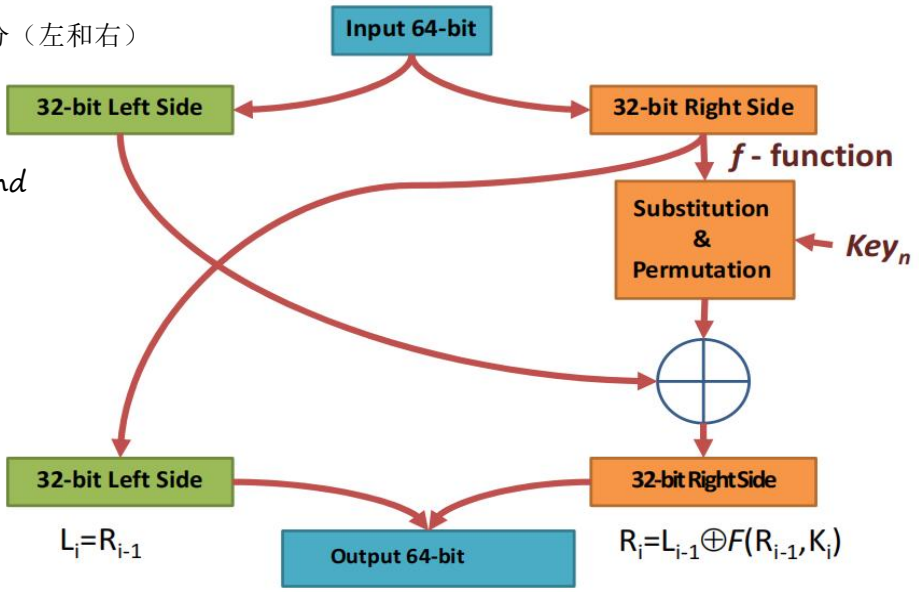
• First the plaintext passes through an initial permutation (T) 首先，明文通过一个初始排列(T)

• The plaintext (ciphertext) is divided in two parts (Left and Right)明文（密文）分为两部分（左和右）

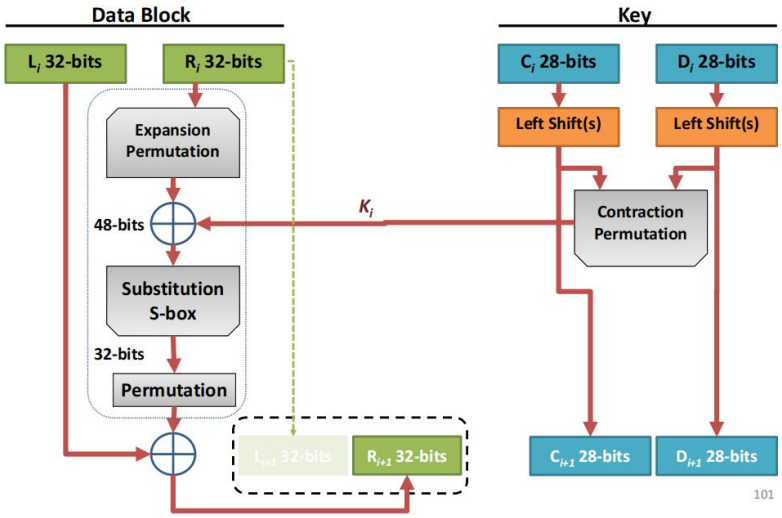
(2)

One Round

in DES



(3)DES: Substitution and Transposition



<1>Permutations (transposition)

- Example with a 6-bit block. Note this is not how it is done in DES as the block sizes are different.具有6位块的示例。注意，这不是在DES中完成的，因为块大小不同。

Input 6-bits	1	2	3	4	5	6
Output 6-bits	3	1	4	2	6	5

Permutation

Input 6-bits	1	2	3	4	5	6		
Output 8-bits	1	2	4	3	4	3	5	6

Expansion Permutation

  - **Notation:**
    - Permutation (3,1,4,2,6,5)
    - Expansion Permutation (1,2,4,3,4,3,5,6)

  - In DES the expansion permutation is from 32-bits to 48-bits.在DES中，扩展排列是从32位到48位

<2>S-box (Substitution)

- Take 6-bits block $b_0\ b_1\ b_2\ b_3\ b_4\ b_5$
- Take the first and last bit, $b_0\ b_5$, this represents a binary number (from 0 to 3 in decimal), let call this number row.(2的2次幂)行
- Take the rest of the bits, $b_1\ b_2\ b_3\ b_4$, this represents a binary number (from 0 to 15), call this number the column.(2的4次幂) 列
- Use the row and column value to read the number in the S-box.使用行和列值来读取S字框中的数字。
  This number is the output of the S-box, the substitution这个数字是S-box的输出，即substitutiuon

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	15	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	2	14	10	0	6	13

Notice that we put the row and columns and the table entries using decimal numbers (instead of binary)请注意，我们使用十进制数字（而不是二进制数字）来放置行、列和表条目

Example:

- Suppose that the binary number is 010110
- The first and last bits are 00, in decimal = 0
- The rest of the bits are 1011, in decimal = 11
- Use the table to find row 0, column 11

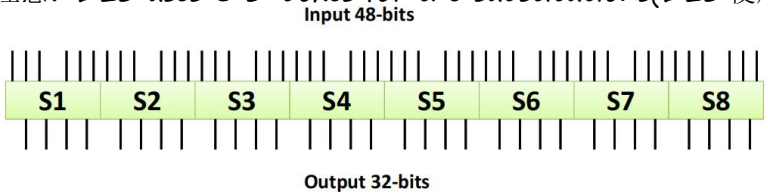
二进制首尾 b0,b5，组合换成十进制对应行
中间部分，组合换成十进制对应列
找到对应行列的单元格

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	15	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	2	14	10	0	6	13

- The entry value is 12 which in binary is 1100.
- The output of the S–box is 1100

把单元格里的数字换成二进制
输出二进制（6→4）

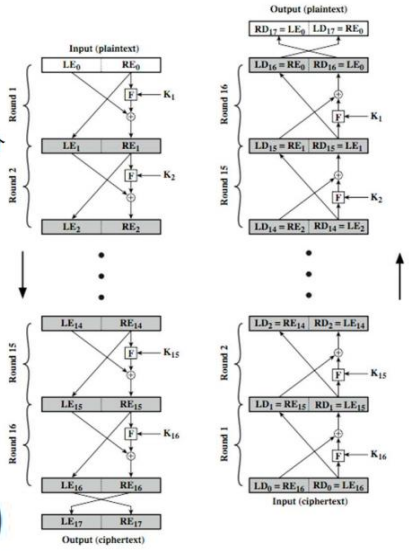
注意：*DES uses 8 S-boxes for the substitutions*(DES 使用 8 个 s-box 来进行替换)



48/6=8
8×4=32

(4)Key-generation

- The algorithm expects a 64-bit long key算法希望64位key
- Every 8-bits of this key is ignored (giving 56-bit key)8位将被忽略(56位）
- The key bits are subjected to a permutation key bits进行排列
- The 56-bit key is split into two parts C_i and D_i ; each of 28-bits long.分两部分
- At each round C_i and D_i are subject to a circular left shift
  在每一轮中，Ci和Di都要向左进行环移
  $b_{27}b_{26}...b_1b_0 \leftarrow b_0b_{27}...b_2b_1$
  (The number of bits shifted depends on the round)
  移动位数取决于几轮
- The sub-key is submitted to a contraction permutation (48-bit output)
  sub-key提交到收缩排列（48位输出）



Notation:

迭代结果： $h_i : (R_i, L_i) \rightarrow (L_{j-1} \oplus f(R_i, K_i), R_i)$

(5)The strength of DES

- **There are two concerns: ????**

– *Cryptanalysis by exploiting the characteristics of the algorithm. However, there are relatively few weaknesses in the algorithm.*利用该算法的特点进行密码分析。然而，该算法的弱点相对较少。

– *The key length:*

Key size in bits	Number of different keys	Time required at 10^6 Decryptions/μs
32	2^{32}	2^{31}μs=2.15ms
56	2^{56}	2^{55}μs=10hrs
128	2^{128}	2^{127}μs=5.4X10^6 yrs
168	2^{168}	2^{167}μs=5.9X10^{30} yrs

不建议 56 位 key，不够安全

4. Double DES

(1)

- Encrypt the same plaintext multiple times using DES with different keys.使用带有不同密钥的DES多次加密相同的明文。
- If simple DES is using a key of 56-bits then the keyspace consists of 2^{56} keys.如果简单的DES使用56位的密钥，那么密钥空间，由2的56次幂组成
- Notation:
  - $E_k(m)$ is the encryption function E with key K and m is the message.
- Double DES will be $E_{K1}(E_{K2}(m))$, where K_1 and K_2 are the keys.

Q: If the keys are of length 56-bits then it seems that in double DES the key space consist of 2 的 112 次幂 keys.？？

如果 key 的长度为 56 位，那么在双 DES 中，key 空间似乎由 2112 个键组成？

Ans：However, this is not true, double DES has the security level of a 57-bit key.

但是，这不是真的，双 DES 具有 57 位密钥的安全级别。相加

(2)Meet-in-the-middle attack(黑恶攻击方式)

- Alice and Bob are going to use double DES
- They know the keys K_1 and K_2.
- Notation:
  - E means encryption and D means decryption.
- Alice sends to Bob the encrypted message $c = E_{K1}(E_{K2}(m))$.
- Bob decrypts the message $m=D_{K2}(D_{K1}(c))$.
- Alice and Bob believe that Eve (the hacker) will need to discover both keys K_1 and K_2 by brute force to decrypt the message.
- Eve has intercepted the message m and $c = E_{K1}(E_{K2}(m))$.
- She wants to find K_1 and K_2 .
- She computes $E_K(m)$ for all possible keys and stores the results in a list.
- She computes $D_K(c)$ for all possible keys and stores the results in a list
- She compares the two lists, and looks for a match
- If she found a match, then Eve knows K_1 and K_2.

5.Triple DEA (TDEA)

(1)• **TDEA uses three keys executions of the DES algorithm**

$c = DES_{K3}(DES_{K2}^{-1}(DES_{K1}(m)))$

where c = ciphertext, m = plaintext

- **Notation:**
  - $DES_K(X)$ = encryption of X using key K
  - $DES_K^{-1}(X)$ = decryption of X using key K

(2)• **Decryption is achieved using**

$$m = DES_{K1}^{-1}(DES_{K2}(DES_{K3}^{-1}(c)))$$

- **Key length 168-bits long**

四. The Advanced Encryption Standard（AES）

1.

- Rijndael is an iterated block cipher. Each intermediate cipher result is called a '**state**'.
  Rijndael是一个迭代的块密码。每个中间的密码结果都被称为"状态"
- Rijndael can operate over a variable-length block using variable-length keys; (128-,192-,256- bit).
  Rijndael可以使用可变长度键在可变长度块上进行操作；（128、192、256位）。
- AES only supports a 128-bit block size. AES只支持128位的块大小
- The algorithm is written so that block length and/or key length can easily be extended in multiples of 32 bits.该算法使得块长度和/或密钥长度可以很容易地扩展到32位的倍数
- Does not use a Feistel structure as it process the entire data block in parallel during each round using substitutions and linear transformations.不使用Feistel结构，因为它在每一轮过程中使用替换和线性转换并行处理整个数据块。
  - In the classic Feistel structure, half of the data block is used to modify the other half of the data block, and then the halves are swapped.在经典的Feistel结构中，数据块的一半用于修改数据块的另一半，然后交换这一半。

2.The cipher Rijndael

- An initial round - key addition;
- N_{r-1} rounds;
- A final round.

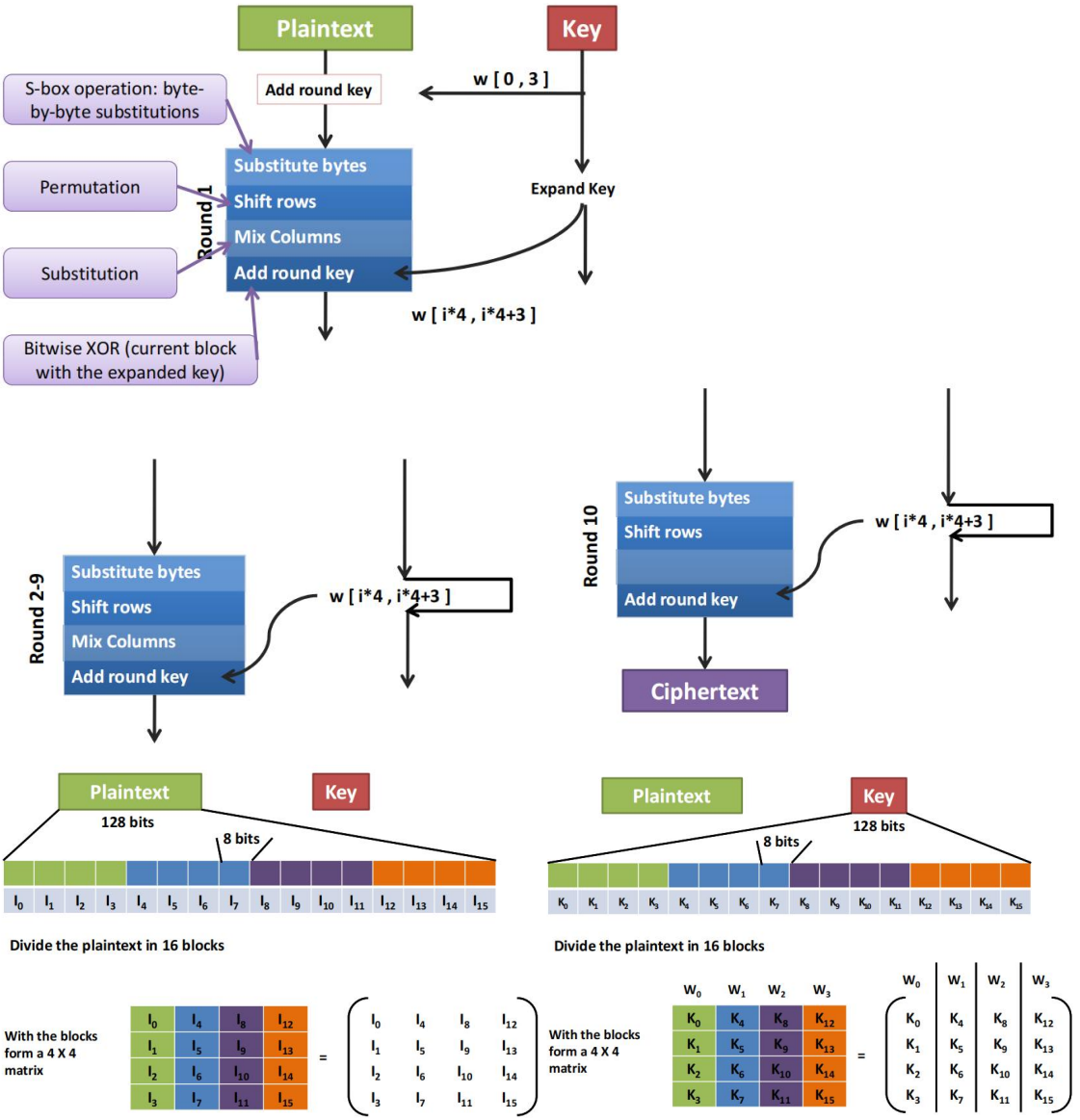
Characteristics
- Immune from all known attacks.
- Fast/compact on various platforms
- Design simplicity.

- In pseudo code (taken from the revised AES proposal)

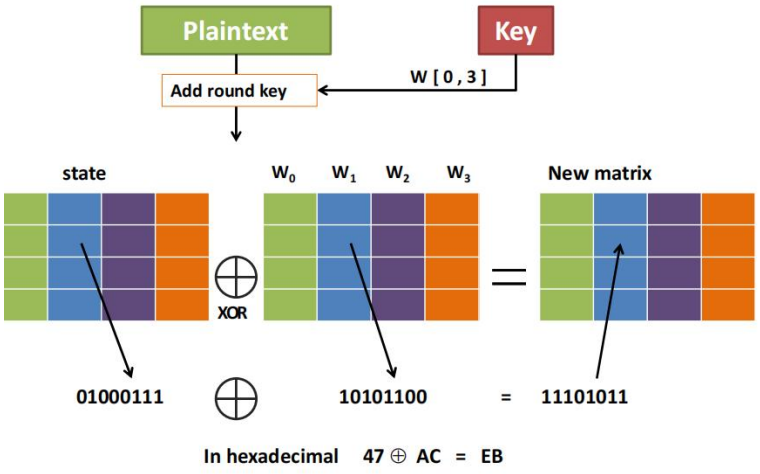
```
Rijndael(State,CipherKey)
 {
 KeyExpansion(CipherKey,ExpandedKey);
 AddRoundKey(State,ExpandedKey);
 For(i=1; i<Nr; i++)
 Round(State,ExpandedKey + Nb*i);
 FinalRound(State,ExpandedKey + Nb*Nr);
 }
```

Key Size (Bits)	128	192	256
Block size (Bits)	128	128	128
Number of rounds	10	12	14
Round Key Size (Bits)	128	128	128
Expanded Key Size (Bytes)	176	208	240

Typical AES parameters

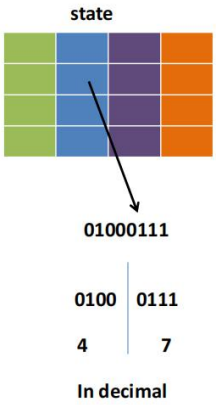


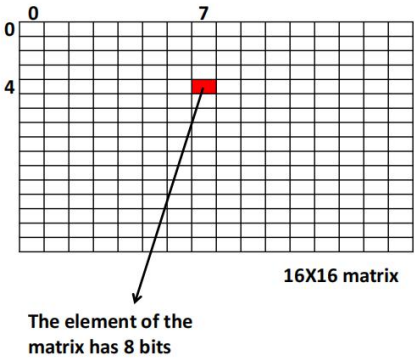
(1)Add round key



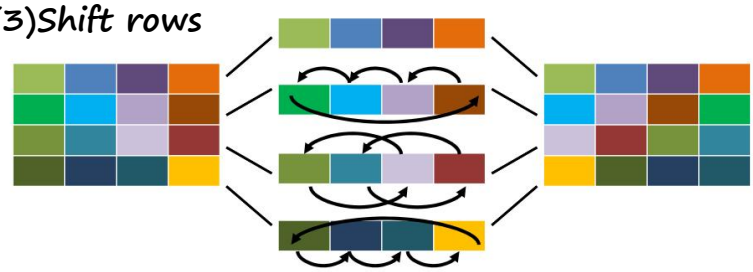
In hexadecimal 47 ⊕ AC = EB

(2)Substitute bytes





(3)Shift rows



First row stays the same第一行不变
Second row, 1-byte circular left shift
第二行都向左移一个字节
third row, 2-byte circular left shift
第三行，向左移动两个字节
Forth row, 3-byte circular left shift
第四行，都向左移动三个字节

左 1 向左 1 个字节——>右 1

(4)Mix Columns

- The mixing of columns is obtained using a matrix multiplication (in the field GF(2^8) *GF = Galois* field)
列的混合是通过矩阵乘法得到的

$$\begin{pmatrix} n_{0,0} & n_{0,1} & n_{0,2} & n_{0,3} \\ n_{1,0} & n_{1,1} & n_{1,2} & n_{1,3} \\ n_{2,0} & n_{2,1} & n_{2,2} & n_{2,3} \\ n_{3,0} & n_{3,1} & n_{2,3} & n_{3,3} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{2,3} & S_{3,3} \end{pmatrix}$$

Where 01, 02 and 03 are in hexadecimal (in binary are 01, 10 and 11 respectively) and n_i denotes the new 'State'.

- **The multiplication is obtained by the sum of multiplying one column by one row (in the field *GF(2^8)*)**一列乘一行相加
- **Example:**

$$n_{0,0} = (2 \bullet S_{0,0}) \oplus (3 \bullet S_{1,0}) \oplus S_{2,0} \oplus S_{3,0}$$

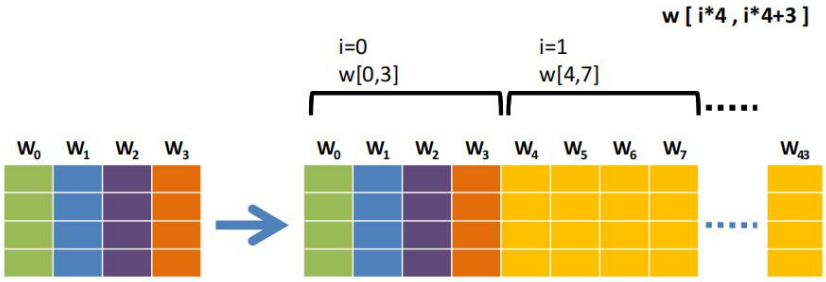
- **The multiplication using • is as follows:**
If the $S_{i,j} = (b_7,b_6,b_5,b_4,b_3,b_2,b_1,b_0)$ then

$$(2 \bullet S_{i,j}) = \begin{cases} (b_6,b_5,b_4,b_3,b_2,b_1,b_0,0) & \text{if } b_7 = 0 \\ (b_6,b_5,b_4,b_3,b_2,b_1,b_0,0) \oplus (00011011) & \text{if } b_7 = 1 \end{cases}$$

and $(3 \bullet S_{i,j}) = S_{i,j} \oplus (2 \bullet S_{i,j})$

See next slide

(5)Add round key



- This slide explains the algorithm used to expand the key.

(6)Key expansion

- SubWord = Byte Substitution using the S box
- RotWord = One-byte circular left shift
- Rcon = 'round' constant (given $r(i) = 00000010^{(i-4)/4}$)

```
KeyExpansion(byte key[16], word[44])
  { word tmp;
  for(i=0;i<4;i++)
   w[i]=(key[4*i],key[4*i+1],key[4*i+2],key[4*i+3]);
  for(i=4;i<44;i++){
   tmp=w[i-1];
   if(i%4==0) tmp=SubWord(RotWord(tmp)) XOR Rcon[i/4];
   w[i]=w[i-4] XOR tmp;
  }
  }
```

If an adversary tries to break the algorithm by searching the key space, then he/she would need to try 2^{100} keys – instead of 2^{128}.

其他算法:

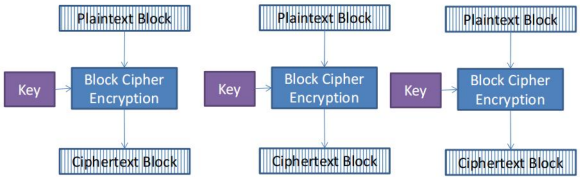
Algorithm	Key Size	Number of Rounds	Mathematical operations	Applications
IDEA	128 bits	8	XOR, addition, multiplication	PGP
Blowfish	Variable to 448 bits	16	XOR, variable S-boxes, rotation	
RC5	Variable to 2048 bits	Variable to 255	Addition, subtraction, XOR, rotation	
CAST - 128	40 to 128 bits	16	Addition, subtraction, XOR, rotation fixed S-boxes	PGP

五. Modes of Operation

- **A Technique for improving the effect of a cryptographic algorithm, or to make it compatible with various applications.**一种改进加密算法的效果，或使其与各种应用程序兼容的技术
  (Four modes)
- **They enable improving the encryption of block ciphers using the same key.**
  - A block cipher processes one block of data at a time, using the same key.
  - For example, in **DES,** the use of the same key would produce the same ciphertext for similar plain texts. THIS SHOULD BE AVOIDED.例如，在DES中，使用相同的键将为类似的纯文本产生相同的密文。这应该避免。
  - This mode of operation is known as "ECB" – See next slide.

1.Electronic Code Book (ECB)

- A block cipher processes one block of data at a time, using the same key.
一个块密码使用相同的key一次处理一个数据块
- Example:
  - **DES:** This mode of DES algorithm should be avoided as far as possible. Why?



- For DEA and TDEA the block length is 64-bits.
- If the same key is used to encrypt the plaintext then there is a unique ciphertext for every 64-bit block of plaintext.如果使用相同的密钥来加密明文，那么每一个64位的明文块都有一个唯一的密文。
- The codebook is the collection of all the unique plaintext, ciphertext blocks.代码本是所有独特的明文，密文块的集合。
- Identical plaintext blocks result in identical ciphertext blocks.相同的明文块会产生相同的密文块。
- If the ciphertext is highly structured a cryptanalyst can use these regularities to break the code.如果密文是高度结构化的，那么密码分析人员可以使用这些规律来破坏代码。

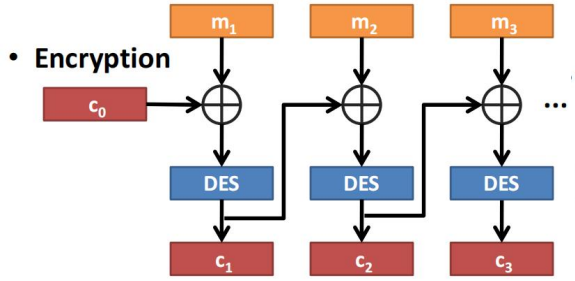
2.Cipher Block Chaining (CBC)

*The encryption depends on the encryption's history. If c0 is an initialisation block agreed among partners.*加密方式取决于该加密方式的历史记录。如果 *c0* 是合作伙伴之间同意的初始化块。

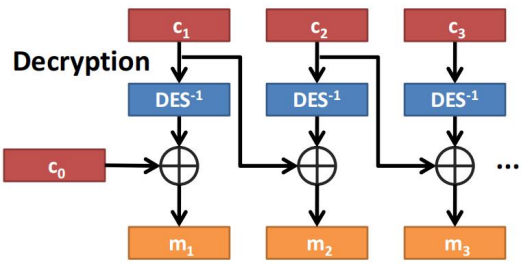
*Same as ECB, i.e. One key, but the input is chained to the previous key –making it stronger than before.*与 *ECB* 一样，即一个 *key*，但输入被链接到前一个键，使其比以前更强大

Encryption	Decryption
$c_1 = DES(m_1 \oplus c_0)$	$m_1 = DES^{-1}(c_1) \oplus c_0$
$c_2 = DES(m_2 \oplus c_1)$	$m_2 = DES^{-1}(c_2) \oplus c_1$
$c_3 = DES(m_3 \oplus c_2)$	$m_3 = DES^{-1}(c_3) \oplus c_2$
…	…

- **Encryption**



Decryption



3.Cipher feedback (CFB) mode

• CFB converts DES into a stream cipher. If the unit of transmission is j-bits (i.e. j=8 bits) CFB 将 DES 转换为流密码。如果传输单位为 j 位（即 j=8 位）

– Start with an initial vector (iv) (given)从初始向量（iv）开始（给定）

– Shift j bits 移动 j 位

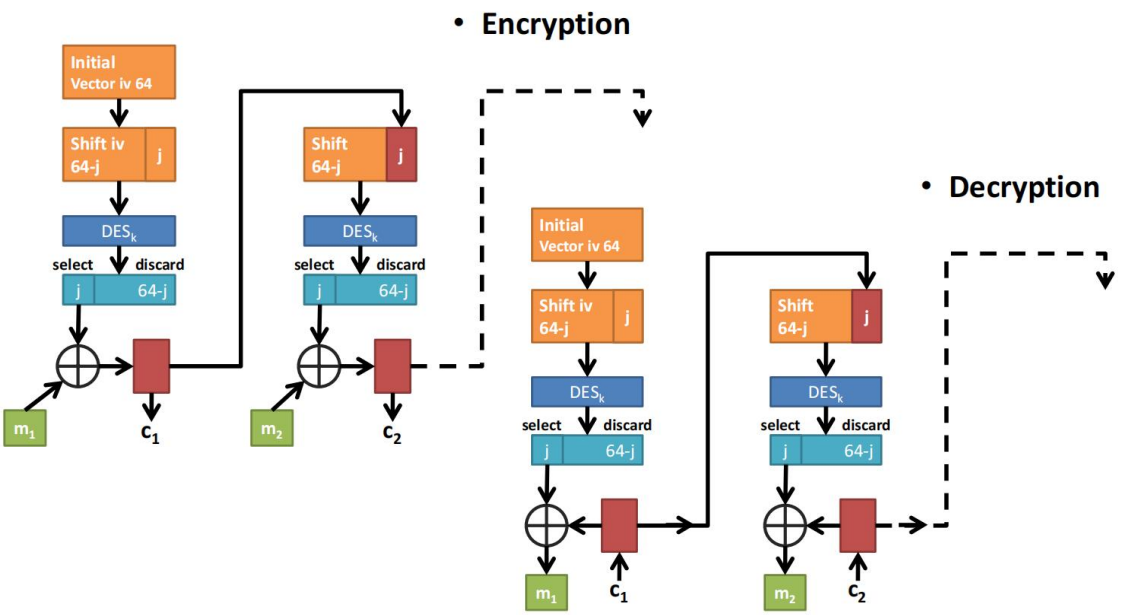
– Encrypt using DES 使用 DES 加密

– Select first j bits 选择第一个 j 位

– XOR with the j bits of the message XOR 与消息的 j 位

– Use the encrypted message as new iv 使用加密的消息作为新的 iv

If j bit inputs were used, then the output will only need j bits→Efficient transmission capacity.如果使用了 j 位输入，那么输出将只需要 j 位→的有效传输容量。



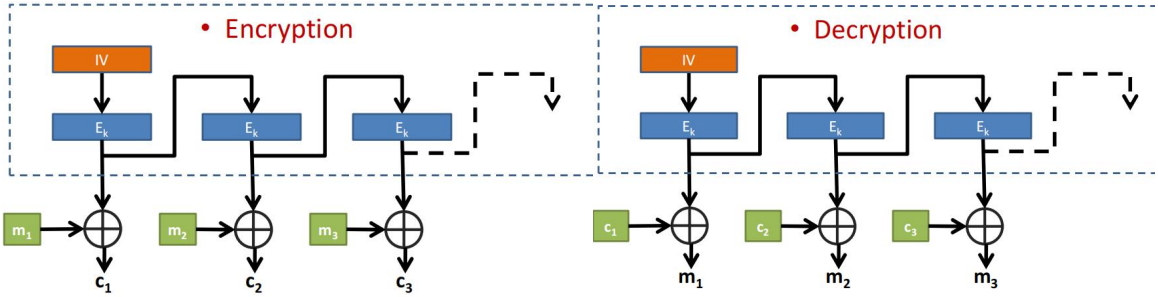
注意：Error Propagation:错误传播

– For an initial block of 64 bits, if an error bit occurs, it propagates to the next 8 blocks. 对于 64 位的初始块，如果出现错误位，它将传播到 接下来的 8 个块。

• The reason is that at each step of the CFB shifts the initial value 8 bits, and it would take 8 rounds of CFB to remove the corrupted bits.原因是在 CFB 的每一步，初始值移动 8 位，需要 8 轮 CFB 才能去除损坏的位。

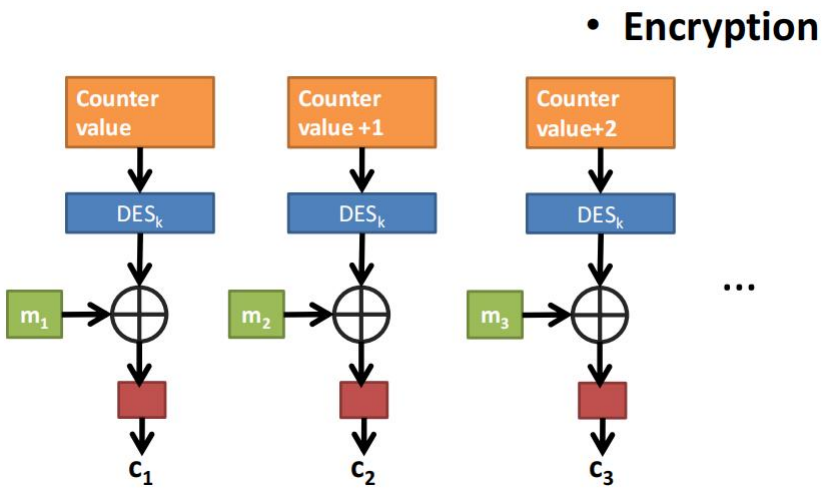
4.Output feedback mode (OFB)

- Unique IV for each use.
- Compared with Cipher Feedback Mode, Output Feedback Mode avoids error propagation.与CFB相比，OFB避免了错误的传播。
- Transforms a block cipher into a stream cipher.将块密码转换为流密码
- Can be computed in advance.可以提前计算出来
- Parallel processing is possible:可以并行处理
  - The block cipher operations may be performed in advance, allowing the final step to be performed in parallel once the plaintext or ciphertext is available.块密码操作可以预先执行，一旦明文或密文可用，就允许并行执行最后一个步骤。 148



5.Counter mode (CTR)

- Also known as
  - Integer Counter Mode (ICM)
  - Segmented Integer Counter (SIC) mode
- Like OFB, turns a block cipher into a stream cipher.与OFB类似，将块密码转为流密码
- It generates the next keystream block by encrypting successive values of a 'counter'.通过加密一个"计数器"的连续值来生成下一个密钥流块
- Increased applications
  - Efficient (HW & SW)
  - Simplicity and Strength



总结:

Mode	Description	Application
ECB	Block of 64 bits are encoded independently using the same key	- Secure transmission of single values (e.g. Key)
CBC	Input is XOR'ed with the next and previous plaintext ciphertext, respectively.	- Generic block transmission - Authentication
CFB	J bits inputs. Previous ciphertext is used in encryption, then XOR'ed with plaintext.	- General stream transmission - Authentication
OFB	Like CFB, but input is the DES output	- Stream transmission/noisy channel(e.g. Satellite comms.)
CTR	Input XOR'ed with encrypted couter.	- Block transmission - High-speed.

六. Key Distribution

- The block ciphers security depends on the secrecy of the key.
块密码的安全性取决于密钥的安全性

- The weakest part of all existing crypto systems is the key negotiation. Once the key negotiation is broken the encryption is worthless!所有现有加密系统中最薄弱的部分是密钥的谈判。一旦密钥协商被破坏，加密就毫无价值了！

Problems:

– There is no message signature. That is a sender cannot prove to his partner that he has sent the message. (e.g. Important problem in E-commerce)没有消息签名。这是一个发送者无法向他的伴侣证明他已经发送了信息。（如：电子商务中的重要问题）

– The keys have to be negotiated on a channel whose security is higher than the channel used for the normal transmissio

密钥必须在一个安全性高于正常传输所用的信道的信道上进行协商。

– The number of keys. For a network with *n* partners that exchange messages with everyone $n(n-1)/2$ keys are needed. (i.e. If n = 1000 then number of keys = 999 000)密钥的数量。
对于具有n个伙伴的网络，与每个人交换消息，需要n（n-1）/2个密钥。

- Partner *A* selects the key and physically delivered to partner *B*.
A选择密钥并实际交给B
- Third party partner *C* selects the key and physically delivered to *A* and *B*. 第三方C选择密钥并实际交付给A和B
- If *A* and *B* have previously and recently used a key, *A* (or *B*) can transmit a new key to the other, encrypted using the old key.
如果A和B以前和最近使用过一个密钥，A（或B）可以将一个新密钥传输，并使用旧密钥进行加密。
- *A* and *B* have an encrypted connection to *C*, *C* deliver the new key on the encrypted links to *A* and *B*.
A和B与C有加密连接，C将加密链接上的新密钥传递到A和B。

七. Additional information

- Closure of *F* under + and *
  For all *a*,*b* *belonging to F*, both *a*+*b* and *a*b* belong to *F***

- Both + and * are associative
  For all *a*,*b*,*c* in *F*, *a*+(*b*+*c*) = (*a*+*b*)+*c* and *a(*b***c*) = (*a***b*)**c***

- Both + and * are commutative
  For all *a*,*b* belonging to *F*, *a*+*b* = *b*+*a* and *a*b* = *b***a***

- The operation * is distributive over the **For all**
  For all *a*,*b*,*c* belonging to *F*, *a(*b*+*c*) = (*a***b*)+(*a***c*)**
- Existence of an additive identity
  There exists an element 0 in *F*, such that for all *a* belonging to *F*, *a*+0 = *a*

- Existence of a multiplicative identity
  There exists an element 1 in *F* different from 0, such that for all *a* belonging to *F*, *a1 = *a***

- Existence of additive inverses
  For every *a* belonging to *F*, there exists an element –*a* such that *a*+(-*a*) = 0

- Existence of multiplicative inverses
  For every *a* ≠ 0 to *F*, there exists an element a^{-1} in *F* such that *aa^{-1} = 1**

GF(2^8)

- **Every element of the field is of the form**

$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0$

Where b_i is 0 or 1. So $b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0$ is the representation of a byte.

- **Example:**

$(x^7+x^6+x^3+x+1) + (x^4+x^3+x^1) = x^7+x^6+x^4+x$

In binary: 11001011 ⊕ 00011001 = 11010010