北京邮電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

《现代密码学》第三讲

密码学的信息论基础

BUPT ISC 信息安全中心

上讲内容回顾

- 代换密码
- 置换密码
- Hill 密码
- 转轮密码
- 古典密码的惟密文攻击方法

本章主要内容

- Shannon 的通信保密系统
- 熵和无条件保密
- 分组密码设计思想

本章主要内容

北京邮电大学
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- Shannon 的通信保密系统
- 熵和无条件保密
- 分组密码设计思想

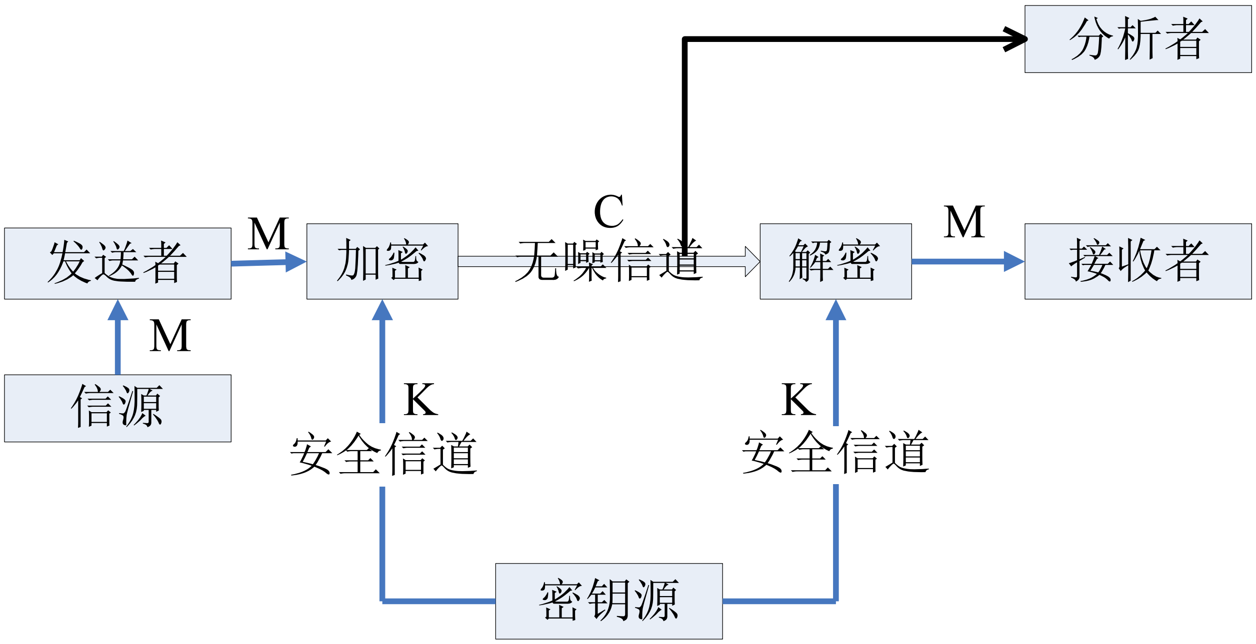
Shannon 通信保密系统

C.E. Shannon （香农） ---- 信息论之父

- 1948, A mathematical theory of communication, 奠定了现代信息论的基础.
- 1949, Communication theory of secrecy systems, 定义了保密系统的数学模型, 将密码学由艺术转化为一门科学.

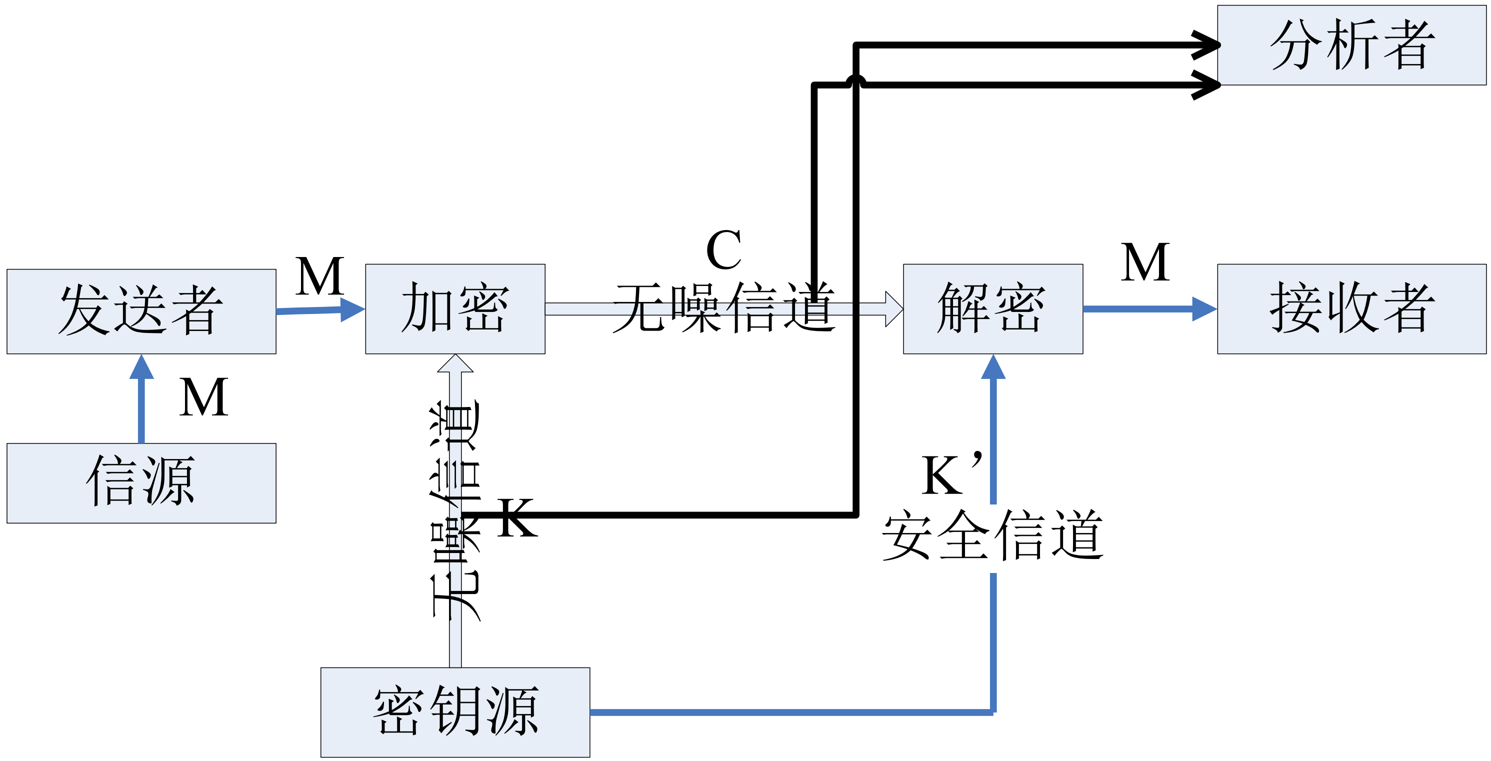
Shannon 通信保密系统

Shannon 的保密通信系统模型：



Shannon 通信保密系统

非对称密码体制：



Shannon 通信保密系统

一个**密码体制**是一个六元组：

$$(\mathcal{P}, \mathcal{C}, \mathcal{K}_1, \mathcal{K}_2, \mathcal{E}, \mathcal{D})$$

其中，

$\mathcal{P}$ -- 明文空间

$\mathcal{C}$ -- 密文空间

$\mathcal{K}_1$ -- 加密密钥空间

$\mathcal{K}_2$ -- 解密密钥空间

$\mathcal{E}$ -- 加密变换

$\mathcal{D}$ -- 解密变换

Shannon 通信保密系统

- 一个加密变换是一个下列形式的映射：

  $$E: M \times K1 \rightarrow C$$

  一般对于给定的 k∈K1，把 E(*, k) 记为 Ek；

- 一个解密变换是一个与加密 E 变换相对应的映射：

  $$D: C \times K2 \rightarrow M$$

  对于给定的 k’∈K2，也把 D(*, k’) 记为 Dk’.

重要原则：

对任一 $k\in\mathcal{K}_1$，都能找到 $k'\in\mathcal{K}_2$，使得

$$\mathcal{D}_{k'}(\mathcal{E}_k(m))=m,\quad \forall\, m\in\mathcal{M}.$$

本章主要内容

- Shannon 的通信保密系统
- 熵和无条件保密
- 分组密码设计思想

熵和无条件保密

定义：

设随机变量 X={x_i ｜ i=1, 2, ..., n}， x_i 出现的概率为 Pr（x_i） ≧0， 且 $\yen_{i=1}^{n}\Pr(x_i)=1$ ， 则 X 的不确定性或熵定义为

$$H(X)=\sum_i p(x_i)\log_a\frac{1}{p(x_i)}\geq 0$$

熵 H(X) 表示集 X 中出现一个事件平均所需的信息量（观察前）； 或集 X 中每出现一个事件平均所给出的信息量（观测后）

熵和无条件保密

从编码的角度来考虑，熵可以理解成用最优的二进制编码形式表示X所需的比特数

规定 $\log_2 0=0$，采用以2为底的对数时，相应的信息单位称作比特

若集X为均匀分布时，即 $p(x_i)=1/n, n \geqq i \geqq 1$，则 $H(X)=\log_2 n$，且若 $H(X) \geqq 0$，当X为确定性的事件时，即X概率分布为 $\Pr(X=a)=1$，则 $H(X)=0$.

熵和无条件保密

定义：

设 $X=\{x_i \mid i=1, 2, \cdots, n\}$， x_i 出现的概率为 $p(x_i) \geqslant 0$ 且 $\sum_{i=1,\cdots,n} p(x_i)=1$；$Y=\{y_i \mid i=1, 2, \cdots, m\}$， y_i 出现的概率为 $p(y_i) \geqslant 0$，且 $\sum_{i=1,\cdots,m} p(y_i)=1$；则集 X 相对于集 Y 的条件熵定义为

$$H(X \mid Y)=\sum_{j=1}^{m} p(y_j) H(X \mid y_j) = -\sum_{j=1}^{m}\sum_{i=1}^{n} p(y_i) p(x_i \mid y_j) \log_2 p(x_i \mid y_j)$$

熵和无条件保密

若将X视为一个系统的输入空间，Y视为系统的输出

空间，在通信中，通常将条件熵 $H(X|Y)$ 称作含糊度，X和Y之间的平均互信息定义为：

$$I(X,Y)=H(X)-H(X|Y)$$

它表示X熵减少量。

熵和无条件保密

定义：

完善保密的（无条件保密的）密码系统（$\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$）

系统满足 $H(\mathrm{P}|\mathrm{C}) = H(\mathrm{P})$ 或 $I(P,C)=0$.

假设攻击者有<u>无限</u>计算资源，仍然不能从密文

得到明文任何信息.

熵和无条件保密

一次一密系统： 设 n 是大于等于 1 的正整数，

$P=C=K=\{0, 1\}^n$，对于密钥 $K\in K$，，$K=\{k_1, k_2, \cdots, k_n\}$.

设明文 P={p1, p2, …, pn}，密文 C={c1, c2, …, cn}.

加密： $\mathcal{E}_K(P)=(p_1\oplus k_1,\ p_2\oplus k_2, \ldots, p_n\oplus k_n)$，

解密： $\mathcal{D}_K(C)=(c_1\oplus k_1,\ c_2\oplus k_2, \ldots,\ c_n\oplus k_n)$.

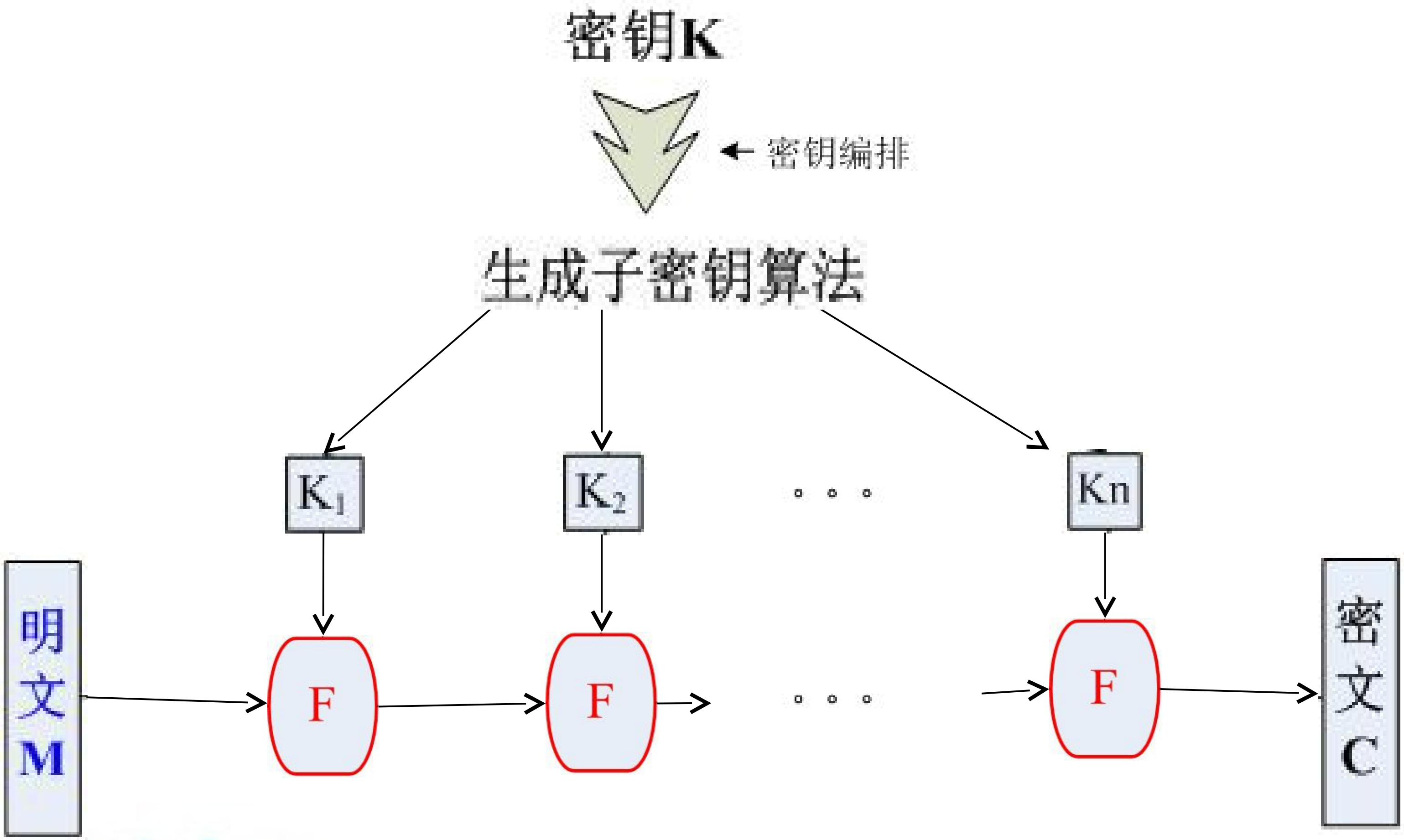
一次一密算法由 Gilbert Vernam 于 1917 年用于报文消息的自动加密和解密，30 年后由 Shannon 证明它不可攻破.

本章主要内容

- Shannon 的通信保密系统
- 熵和无条件保密
- 分组密码设计思想

分组密码设计思想

- 迭代结构（乘积密码）：



分组密码设计思想

北京邮电大学 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 如果密码体制不是幂等的（$F^2 \neq F$），那么多次迭代有可能提高密码体制的安全性.
- 采用迭代结构的优点：软、硬件实现节省了代码（硬件）资源.

分组密码设计思想

- 混淆：明文/密钥和密文之间的关系复杂
- 扩散：明文/密钥的每一个比特都影响密文的每一个比特

主要知识点小结

- Shannon 的通信保密系统
- 熵和无条件保密
- 分组密码设计思想

THE END！