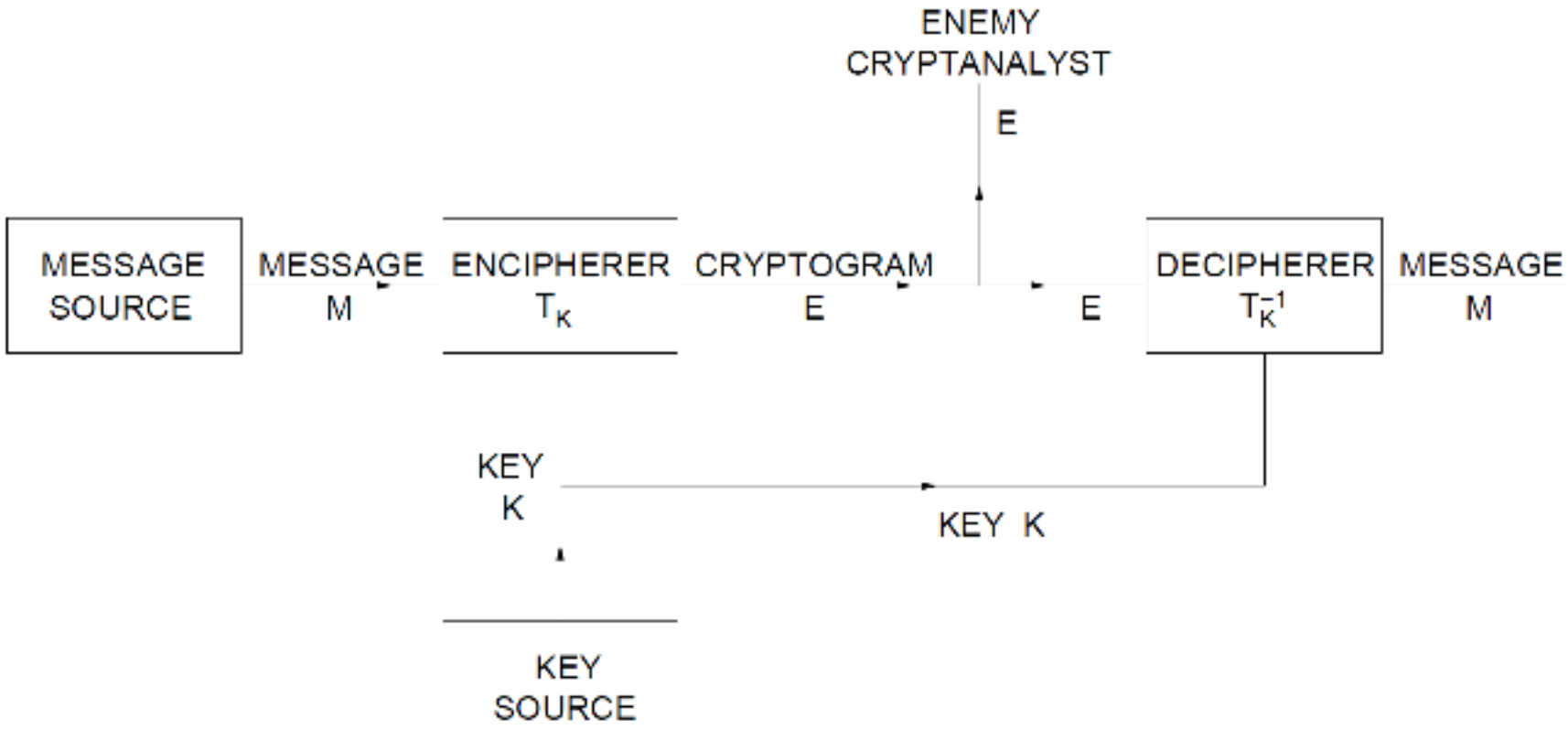
# 末章 信息论和信息安全

- 保密系统的安全性衡量
  - ✓ 完善安全性（无条件安全）：拥有无限计算资源的密码分析者无法破译系统
  - ✓ 计算安全性：利用已有的最好方法来破译该系统所需的资源超过了密码分析者的能力
- 香农的论文“Communication Theory of Secrecy System”，*Bell System Technical Journal*, vol. 28, no. 4, 1949, pp656-715 为私钥密码系统奠定了理论基础。

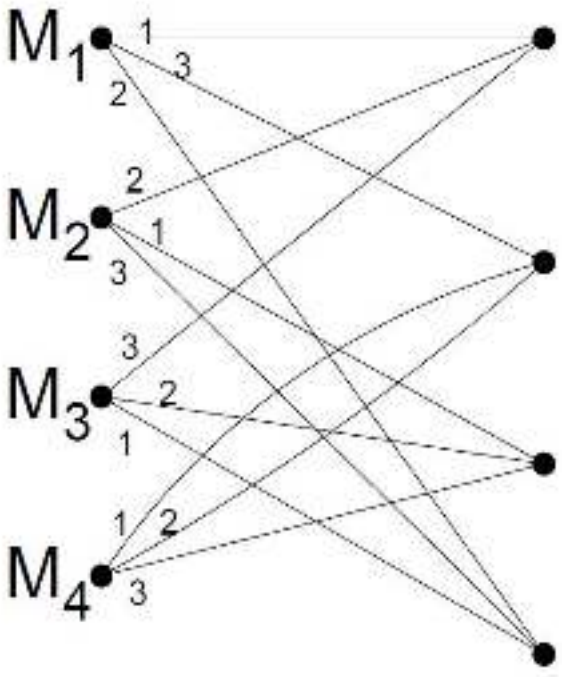
# 保密系统模型


ENEMY
CRYPTANALYST
E
MESSAGE
SOURCE
MESSAGE
M
ENCIPHERER
$T_K$
CRYPTOGRAM
E
E
DECIPHERER
$T_K^{-1}$
MESSAGE
M
KEY
K
KEY K
KEY
SOURCE

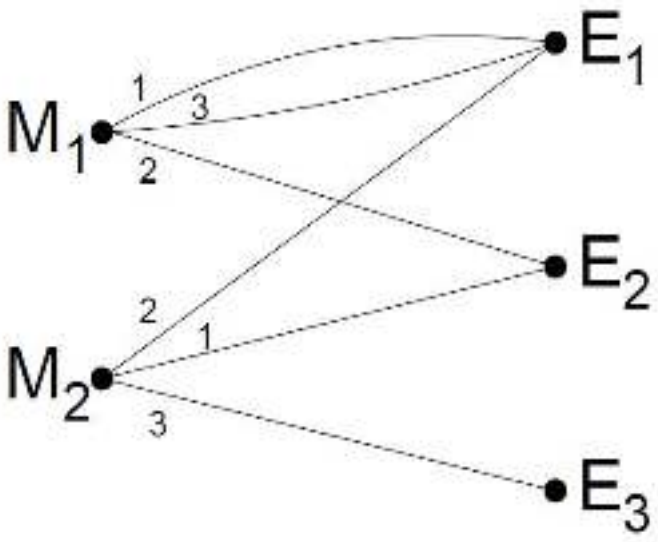
# 保密系统模型

- 明文空间：M
- 密文空间：E
- 密钥空间：K
- 加密算法：$T_K$
- 解密算法：$T_k^{-1}$
- 密码分析者知道系统的统计特性
- 从信息论的观点出发，“加密”可视为增熵的过程,“解密”可视为减熵的过程。
- 加解密过程可以看作是一种编解码过程，研究如何隐蔽消息中的信息内容，使它在传输过程中不被窃听，提高通信系统的安全性。

# 保密系统模型的另一种表示方法




CLOSED SYSTEM




NOT CLOSED

# 完善保密性（perfect secrecy）

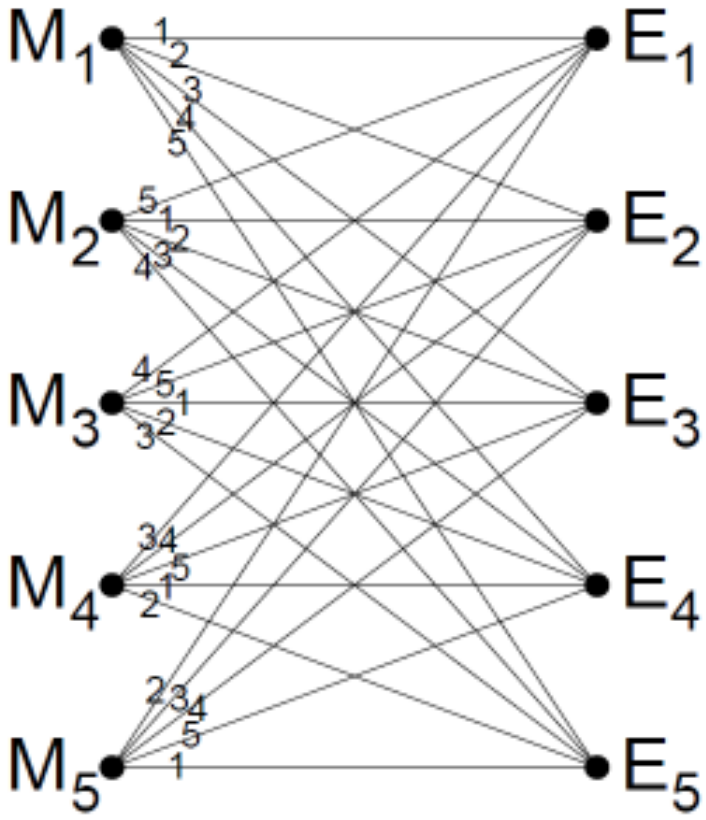
- 明文M的概率分布：P(M)
- 密文E的概率分布：P(E)
- 密钥K的概率分布：P(K)
- 完善保密性的充分必要条件是：

$$P(M|E)=P(M)$$

$$P(E|M)=P(E)$$

- 密钥空间大小不小于明文空间大小

# 完善保密系统



# Equivocation（条件熵）

- Equivocation代表收到密文后对明文或密钥还存在的不确定度：H(M|E), H(K|E)
- Equivocation的性质
  - ✓ $H(M|E) \leq H(K|E)$
  - ✓ H(K|E)=H(M)+H(K)-H(E)
  - ✓ Equivocation和序列长度N有关

# Equivocation的例子

- 简单的字母替代加密

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

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

- ✓ N=1：完善保密系统
- ✓ N=8：保密性较强的系统
- ✓ N=15：保密性较弱的系统
- ✓ N=50：无保密的系统

# 冗余度（Redundancy）

- 冗余度的定义：

$$D_N = \log G - H(M)$$

其中G是所有可能的N长序列明文的个数

- N长序列密文所提供的关于密钥的信息量小于冗余度

$$H(K) - H(K|E) = I(K;E) \leq D_N$$

- 平均冗余度

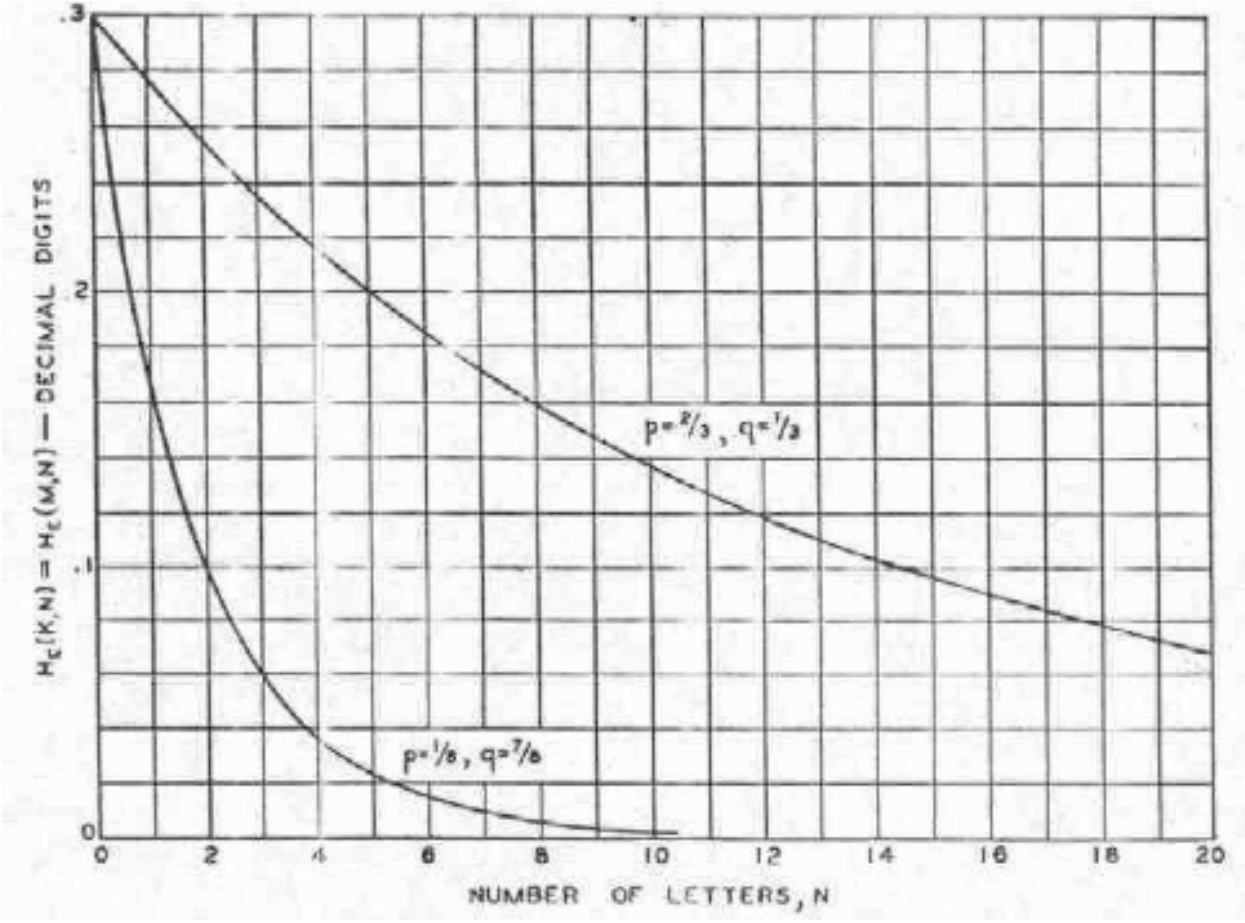
$$D = \frac{D_N}{N}$$

# Equivocation的计算

- 简单的二元字母替代加密
  - ✓ 0，1的概率分别为p和q
  - ✓ H(M|E)=H(K|E)
  - ✓ 密钥等概率分布

$$H_E(K,N) = -\sum_s \binom{N}{s} p^s q^{N-s} \log \frac{p^s q^{N-s}}{(p^s q^{N-s} + q^s p^{N-s})}.$$

# Equivocation的计算



# 唯一解距离（unicity distance）

- 唯一解距离的物理含义：将密钥惟一确定所平均需要的密文长度
- H(K|E)=0
- 唯一解距离为：

$$N = \frac{H(K)}{D}$$

- 唯一解距离和明文的熵有关
- 如何确定唯一密钥：不关心

# 完善保密性和信息论

- 完善保密性的充分必要条件为以下条件之一：
  1. I(M,E)=0
  2. H(M|E)=H(M)
  3. I(K,E)=H(E)-H(M|E)
- 完善保密性的必要条件：

$$H(K) \geq H(E)$$

# 本课程结束!