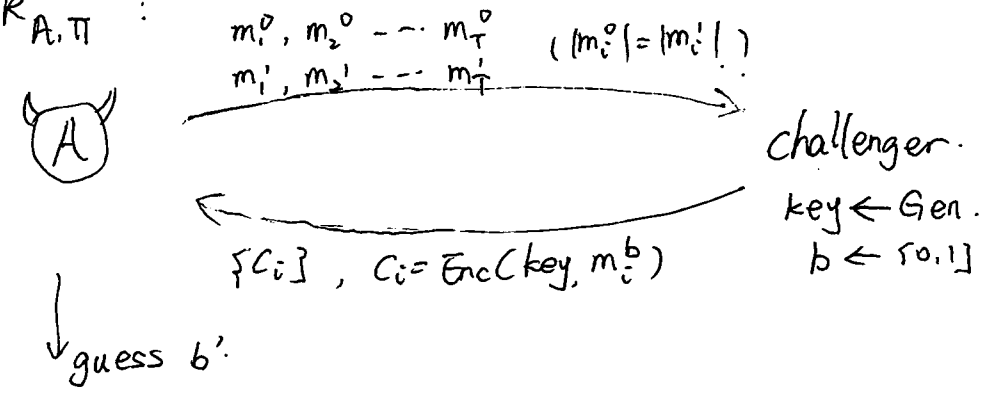
omultiple-msg eavesdropping experiment.

$Priv K^{mult}_{A,\Pi}$:



↓ guess b'.

A' wins iff $b' = b$.

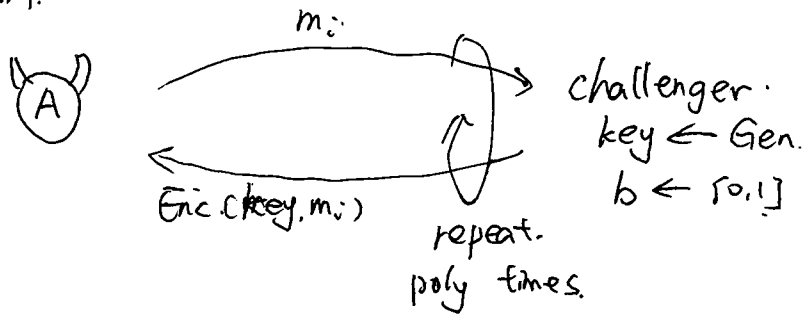
o if $m_1^0 = \cdots = m_T^0$, $m_1^1 \neq \cdots \neq m_T^1$,

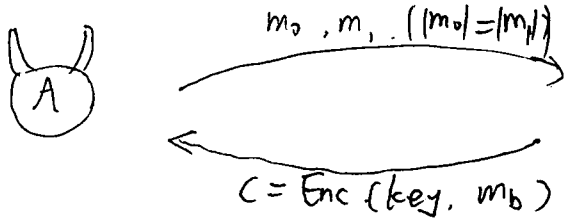
如果 Enc 确定性函数，则 $b=0$ 时，各 c_i 相等；$b=1$ 时，很可能 c_i 不全相等

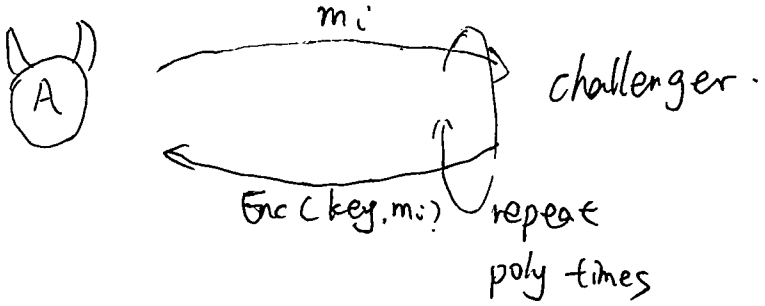
因此考虑安全性时，Enc 必须是 randomized 或 stateful.

, Chosen Plaintext Attack (CPA)

$Priv K^{CPA}_{A,\Pi}$.



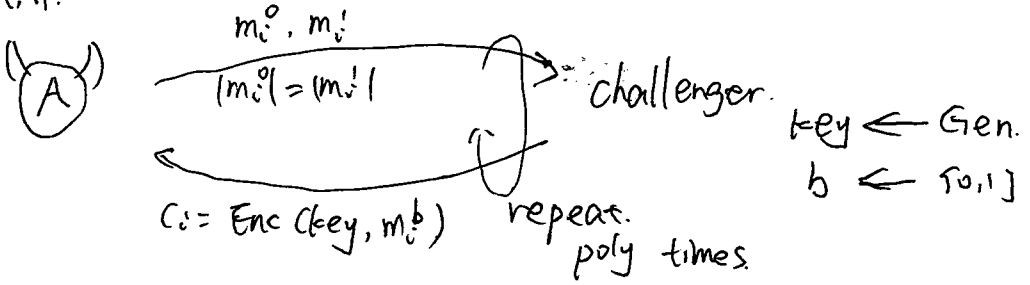




A guess b', A wins iff $b' = b$

, Multi-Msg Chosen Plaintext Attack.

$Priv^{multCPA}_{A,\Pi}$:



A guess b', A wins iff $b=b'$

- CPA 安全性等同于 MultCPA.
  - MultCPA $\geq$ CPA-, 如果 $\exists$ A breaks CPA security, 定义 A', 在 A 除了发送 (m_0, m_1) 的一轮之外的每一轮, 均发送 $m_i^0 = m_i^1 = m_i$, 在 A 发送 (m_0, m_1) 的一轮发送 (m_0, m_1), 则 A' breaks multCPA security.
  - CPA $\geq$ MultCPA.

	$Hybrid_0$ ($b=0$)	$Hybrid_1$	...	$Hybrid_T$ ($b=1$)
challenger:	$Enc(m_1^0)$	$Enc(m_1^1)$		$Enc(m_1^1)$
	$Enc(m_2^0)$	$Enc(m_2^0)$		$Enc(m_2^1)$
	⋮	⋮		⋮
	$Enc(m_T^0)$	$Enc(m_T^0)$		$Enc(m_T^1)$

if $\exists$ A breaks multCPA security.

定义 A': sample $t \leftarrow \{0,1,\cdots T\}$

if $i<t$. A^{III} query m_i^1, challenger return $Enc(m_i^1)$

if $i=t$. A^{III} query m_i^0, m_i^1. challenger return $Enc(m_i^b)$

if $i>t$. A^{III} query m_i^0, challenger return $Enc(m_i^0)$

A' 输出 A^{III} 的 output.

- CPA (和 multCPA) 等价强于 mult-msg eavesdropping experiment.

  假定一个 $\Pi = (Gen, Enc, Dec)$

  定义 $\Pi'(Gen', Enc', Dec')$.

  Gen': $k' \leftarrow (k \xleftarrow{w} Gen \,||\, r \leftarrow \{0,1\}^\lambda)$

  Enc': $Enc'_{(k,r)}(m) = \begin{cases} Enc_k(m) \,||\, r & m \neq r \\ Enc_k(m) \,||\, k & m = r \end{cases}$

  在 CPA security 下, A 只要随机发一个 m 得到 r, 再发送 r 得到 k.
  就可以攻击成功.

- Pseudorandom Function (PRF)

  $f: \{0,1\}^\lambda \times \{0,1\}^{n(\lambda)} \longrightarrow \{0,1\}^{m(\lambda)}$

  ($f(key, input) = output$ or $f_{key}(input) = output$)

  1) f poly-time computable.

  2) f_{key} looks like a random function under oracle access:

  $\forall$ p.p.t. D.

  $$\left| \Pr_{key}[D^{f_{key}(\cdot)}(1^\lambda) = 1] - \Pr_{F:\{0,1\}^n \to \{0,1\}^m}[D^{F(\cdot)}(1^\lambda) = 1] \right| \leq negl.$$

- Pseudorandom Permutation (PRP)

  $f: \{0,1\}^\lambda \times \{0,1\}^n \longrightarrow \{0,1\}^m$.

  1) f_{key} is a keyed permutation.

  2) f, f^{-1} poly-time computable. ($f^{-1}: \{0,1\}^\lambda \times \{0,1\}^m \longrightarrow \{0,1\}^n$)

  3) f_{key} looks like a random function under oracle access

- strong PRP.

  1). 2) 同 PRP.

  3) $$\left| \Pr_{key}[D^{f_{key}(\cdot), f_{key}^{-1}(\cdot)}(1^\lambda) \to 1] - \Pr_{P}[D^{P(\cdot), P^{-1}(\cdot)}(1^\lambda) \to 1] \right| \leq negl.$$

- if f is a PRF, 定义 Π for fixed-length msg:

  Π (Gen, Enc, Dec):

  Gen(1^λ): sample $k \leftarrow \{0,1\}^\lambda$.

  Enc(k, m): sample r.

  $c = (r, f(k,r) \oplus m)$

  Dec(k, (r,c)): $m = c \oplus f(k,r)$

- 上面的 CPA security:

  考虑 Π': Gen': sample $F: \{0,1\}^n \to \{0,1\}^n$

  Enc(F, m): sample r.

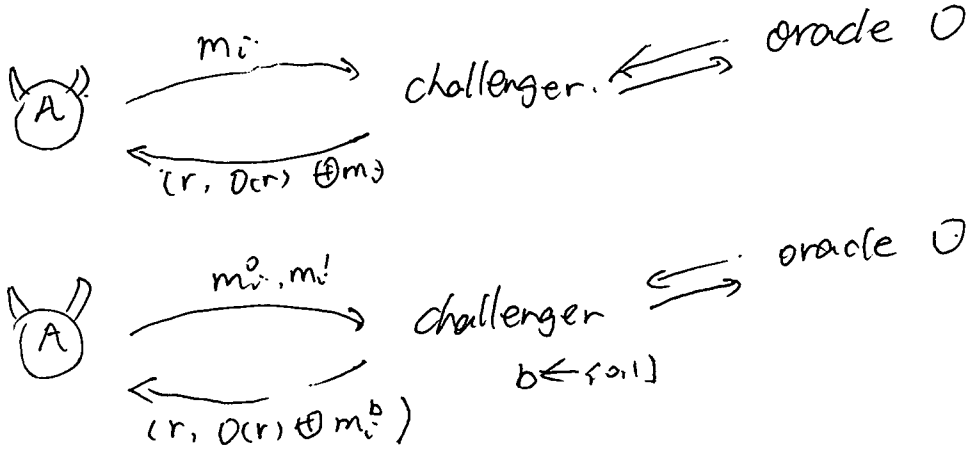
  $c = (r, F(r) \oplus m)$

  Π' 的 security: 由于前若干次查寻 F, 有 $\geq 1-\text{negl}$ 概率, 它们的 r 均不同, 而在该情况下 A 胜率不超过 $\frac{1}{2}$, 故 Π' 是安全的

  如果 $\Pr[\text{PrivK}^{\text{CPA}}_{A,\Pi}(1^\lambda) \to 1] \geq \frac{1}{2} + \frac{1}{\text{poly}}$

  $\Rightarrow \left| \Pr[\text{PrivK}^{\text{CPA}}_{A,\Pi}(1^\lambda) \to 1] - \Pr[\text{PrivK}^{\text{CPA}}_{A,\Pi'}(1^\lambda) \to 1] \right| \geq \frac{1}{\text{poly}}$

  D:



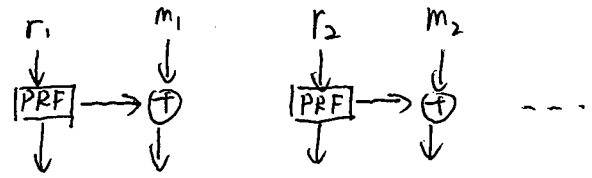
  D 与 f 是 PRF 定义相违背.

- 不固定长度.

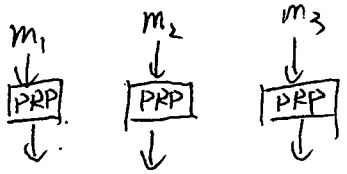
  $\underbrace{x\,10\cdots0}_{\text{长度为}\lambda\text{指数}} = m_1 \| m_2 \| \cdots \| m_\ell$, $|m_i| = \lambda$.

  $\text{Enc}'(k, x) = \text{Enc}(k, m_1) \| \cdots \| \text{Enc}(k, m_\ell)$ (每次使用新 r 独立选取)

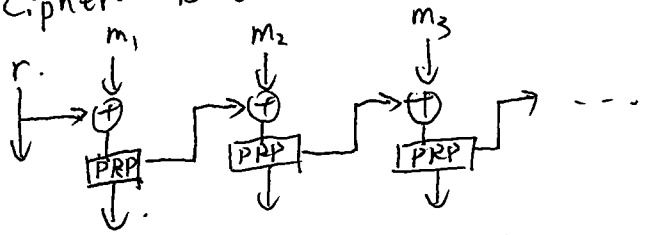
◦ Modes of Block cipher.

1) 

2) Electronic Code Book



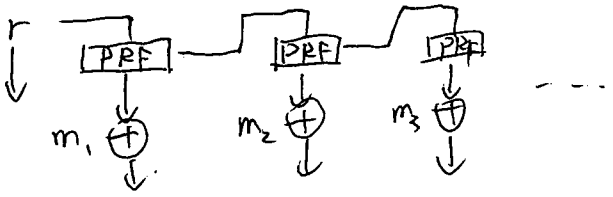
3) Cipher Block Chain.



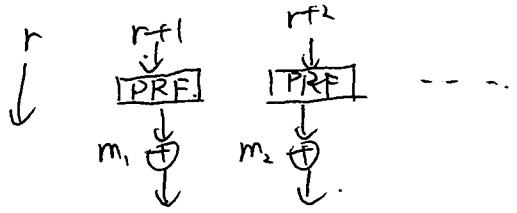
证明其安全性的方式与之前类似，将PRP替换为FC(随机函数)，再利用PRP定义说明两者CPA game胜率差距 ≤ negl

如果将上一次 Cipher Block Chain 中最后一个 output 作为下一次r使用，则没有安全性，

4) output Feedback.



5) Counter.



证明 4), 5) 安全性时，要注意其与 Stream-Cipher 的相似性.

◦ PRF 得出 PRG:

由 $g(seed) = f(0, seed) \| f(1, seed) \| f(2, seed) \| \cdots$

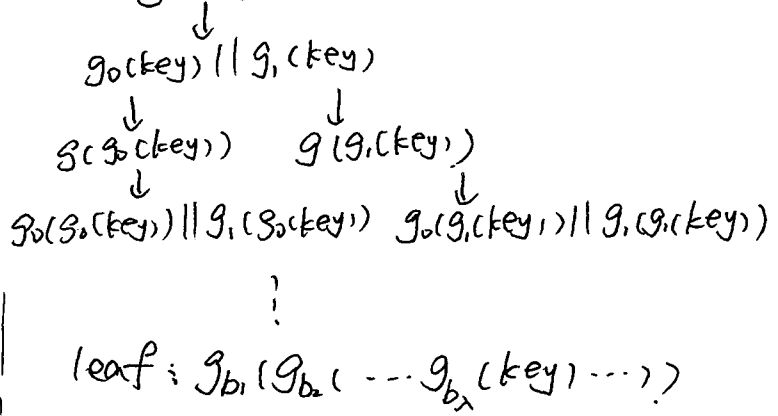
- 由 PRG 得到 PRF.

PRG: $g: \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$.

PRF: $f(key, x)$

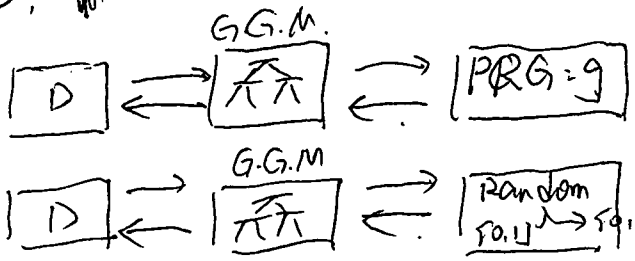
$= g_{x_\lambda}(g_{x_{\lambda-1}}(\cdots g_{x_2}(g_{x_1}(key))\cdots))$

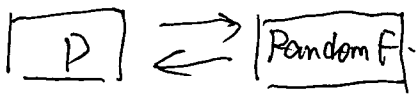
G.G.M.:



若找 G.G.M. 构造出的 f 有 distinguished.

D, ##





，则 D 区分第1个和第3个，和第2个和第3个大概率相同，故 D 区分第1个和第2个.

Hybrid 式：前若干次 query 按 PRG 计算，后若干次使用随机串代替 PRG.