

# W2 4-2 Modes of operation: one time key

## 1、Using PRPs and PRFs

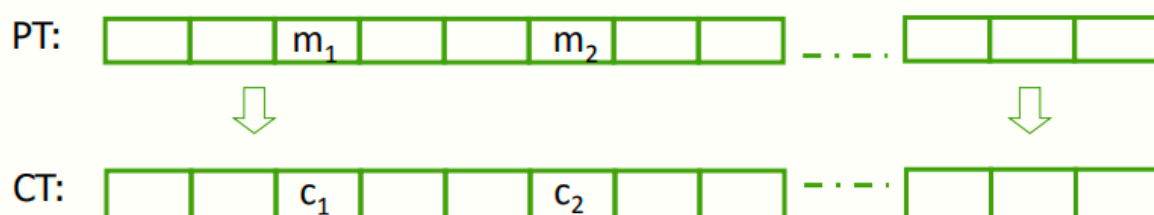
目的：通过安全的PRP构建安全的加密方案，本例中旨在使用块密码来使用一次性密钥来加密

攻击者的能力：只能看到一次性密钥加密后的密文

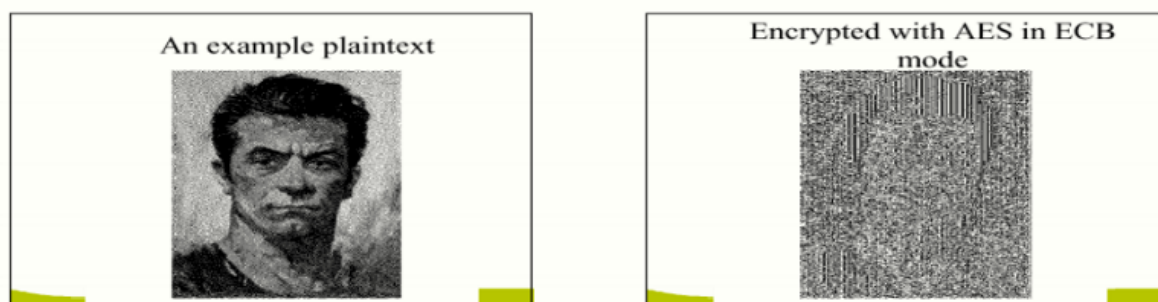
攻击者目标：从CT中提取PT信息（即破坏语义安全）

## 2、Incorrect use of a PRP

ECB模式，流程如下

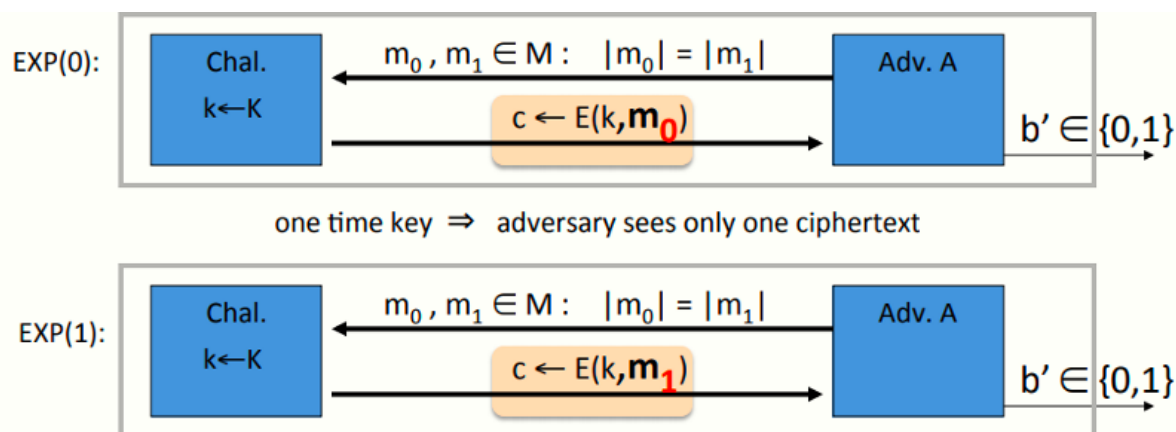


隐性问题：若消息 $m_1=m_2$ ，则加密后的 $c_1=c_2$ ，从而攻击者可以获取一些明文之间的关系，而这些关系不应反应在密文上



若将该模式用于加密图片信息，则可能得到如图结果，尽管没有暴露所有的信息，但是仍能反应出一些人物轮廓

## 3、Semantic Security (one-time key)



$$\text{Adv}_{\text{SS}}[A, \text{OTP}] = \left| \Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1] \right| \text{ should be "neg."}$$

对于OTP而言，攻击者应只能看见CT，因此若要做到语义安全，上述优势 $\text{Adv}_{\text{SS}}[A, \text{OTP}]$ 应可忽略

## 4、ECB is not Semantically Secure

ECB并不是语义安全的，因此ECB模式不应加密超过一个块的信息

## 5、Secure Construction I

Deterministic counter mode from a PRF  $F: \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$

$$E_{\text{DETCR}}(k, m) =$$

$m[0]$	$m[1]$	...	$m[L]$
⊕			
$F(k,0)$	$F(k,1)$	...	$F(k,L)$
-----			
$c[0]$	$c[1]$	...	$c[L]$

(e.g.  $n=128$ )

## 6、Deterministic counter-mode security

定理：对于任给的 $L>0$ ，若 $F$ 为定义在三元组 $(\mathcal{K}, \mathcal{X}, \mathcal{X})$ 上的PRF， $E_{\text{DETCR}}$ 为定义在三元组 $(\mathcal{K}, \mathcal{X}^L, \mathcal{X}^L)$ 上语义安全的密码

特别地，对于任意高效的攻击者攻击 $E_{\text{DETCR}}$ ，存在一高效的PRF攻击者 $B$ ，使得：

$$\text{Adv}_{\text{SS}}[A, E_{\text{DETCR}}] = 2 \cdot \text{Adv}_{\text{PRF}}[B, F]$$

Theorem: For any  $L>0$ ,

If  $F$  is a secure PRF over  $(\mathcal{K}, \mathcal{X}, \mathcal{X})$  then

$E_{\text{DETCR}}$  is sem. sec. cipher over  $(\mathcal{K}, \mathcal{X}^L, \mathcal{X}^L)$ .

In particular, for any eff. adversary  $A$  attacking  $E_{\text{DETCR}}$  there exists a n eff. PRF adversary  $B$  s.t.:

$$\text{Adv}_{\text{SS}}[A, E_{\text{DETCR}}] = 2 \cdot \text{Adv}_{\text{PRF}}[B, F]$$

证明如下：

