Using block ciphers

Using block ciphers

Modes of operation: many time key (CBC)

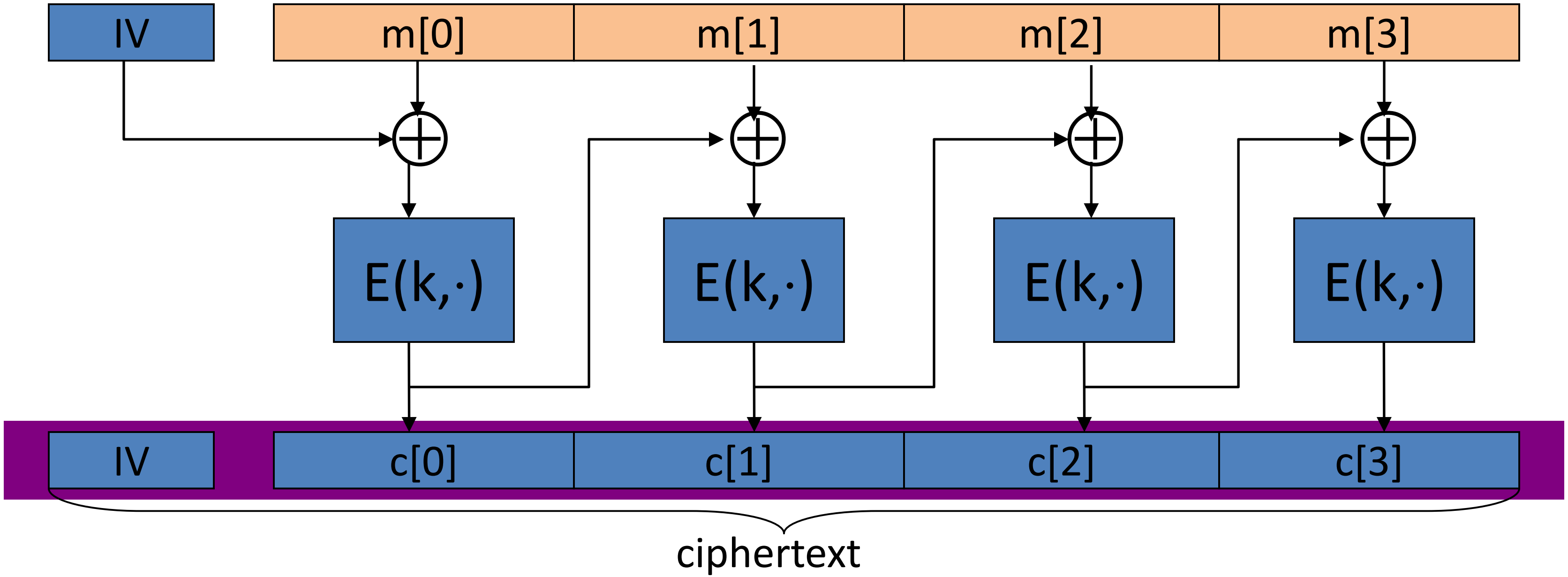
<u>Example applications</u>:

1. File systems: Same AES key used to encrypt many files.
2. IPsec: Same AES key used to encrypt many packets.

Construction 1: CBC with random IV

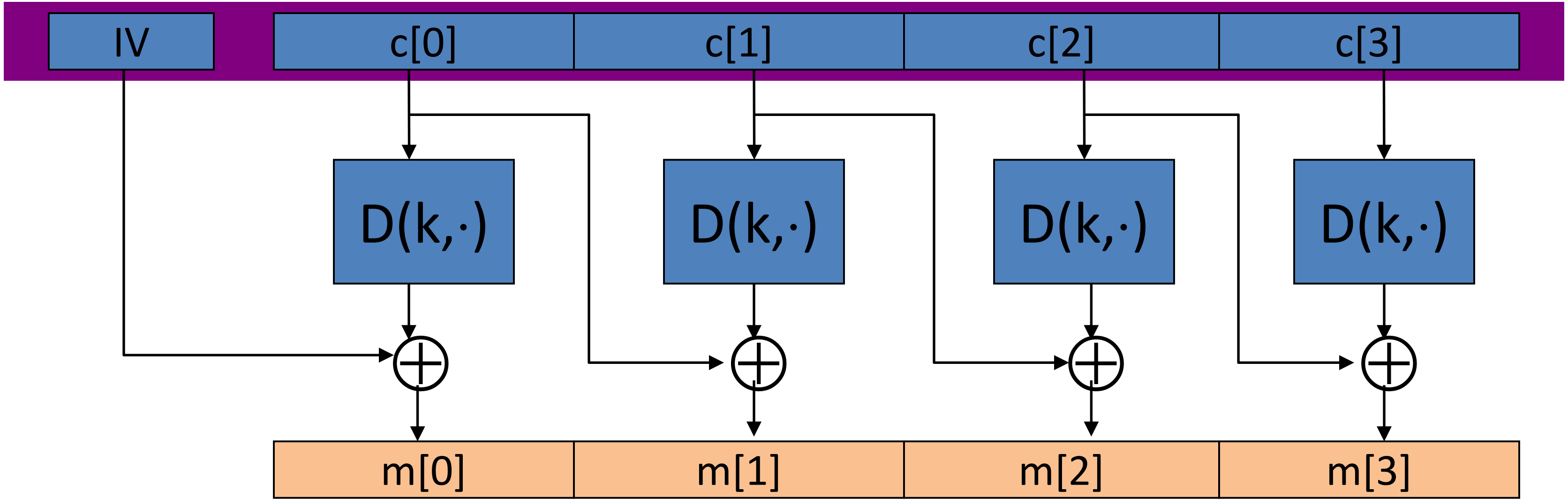
Let (E,D) be a PRP. $E_{CBC}(k,m)$: choose **random** IV∈X and do:

$E: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ $IV \in \{0,1\}^n$



Decryption circuit

In symbols: $c[0] = E\big(k, IV \oplus m[0]\big) \Rightarrow m[0] = D\big(k, c[0]\big) \oplus IV$



CBC: CPA Analysis

<u>CBC Theorem</u>: For any L>0,

Proof in recitation

If E is a secure PRP over (K,X) then

E_{CBC} is sem. sec. under CPA over (K, X^L, X^{L+1}).

In particular, for a q-query adversary A attacking E_{CBC}

there exists a PRP adversary B s.t.:

$$\text{Adv}_{CPA}[A, E_{CBC}] \leq 2 \cdot \text{Adv}_{PRP}[B, E] + \mathbf{2\, q^2\, L^2 / |X|}$$

Note: CBC is only secure as long as $\mathbf{q^2L^2 \ll |X|}$

An example

$$\text{Adv}_{\text{CPA}}[A, E_{\text{CBC}}] \leq 2 \cdot \text{PRP Adv}[B, E] + \mathbf{2\, q^2\, L^2 / |X|}$$

q = # messages encrypted with k , L = length of max message

Suppose we want $\text{Adv}_{\text{CPA}}[A, E_{\text{CBC}}] \leq 1/2^{32}$ $\Leftarrow$ $q^2 L^2 / |X| < 1/2^{32}$

- AES: $|X| = 2^{128}$ $\Rightarrow$ $q\, L < 2^{48}$

  So, after 2^{48} AES blocks, must change key

- 3DES: $|X| = 2^{64}$ $\Rightarrow$ $q\, L < 2^{16}$

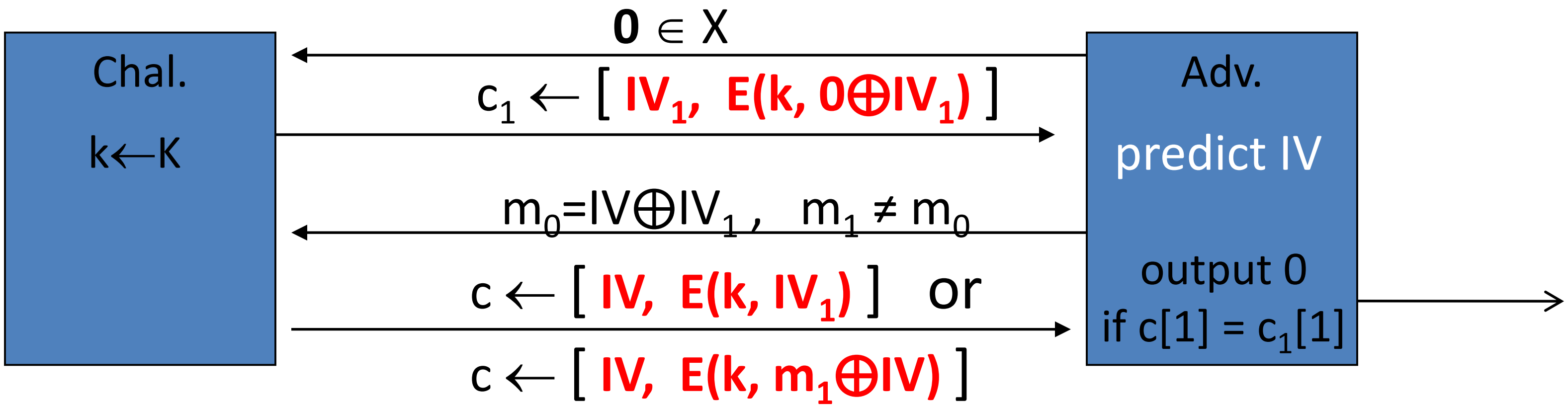
Contrast with asymptotic security

- Guarantees that adversary's advantage is negligible for all "sufficiently" large security parameters
  - Does not provide guidance on what is "sufficiently" large
  - Theoretically more pleasing: less machine dependent

Attack on CBC with predictable IV

CBC where attacker can predict the IV is not CPA-secure !!

Suppose given $c \longleftarrow E_{CBC}(k,m)$ can predict IV for next message

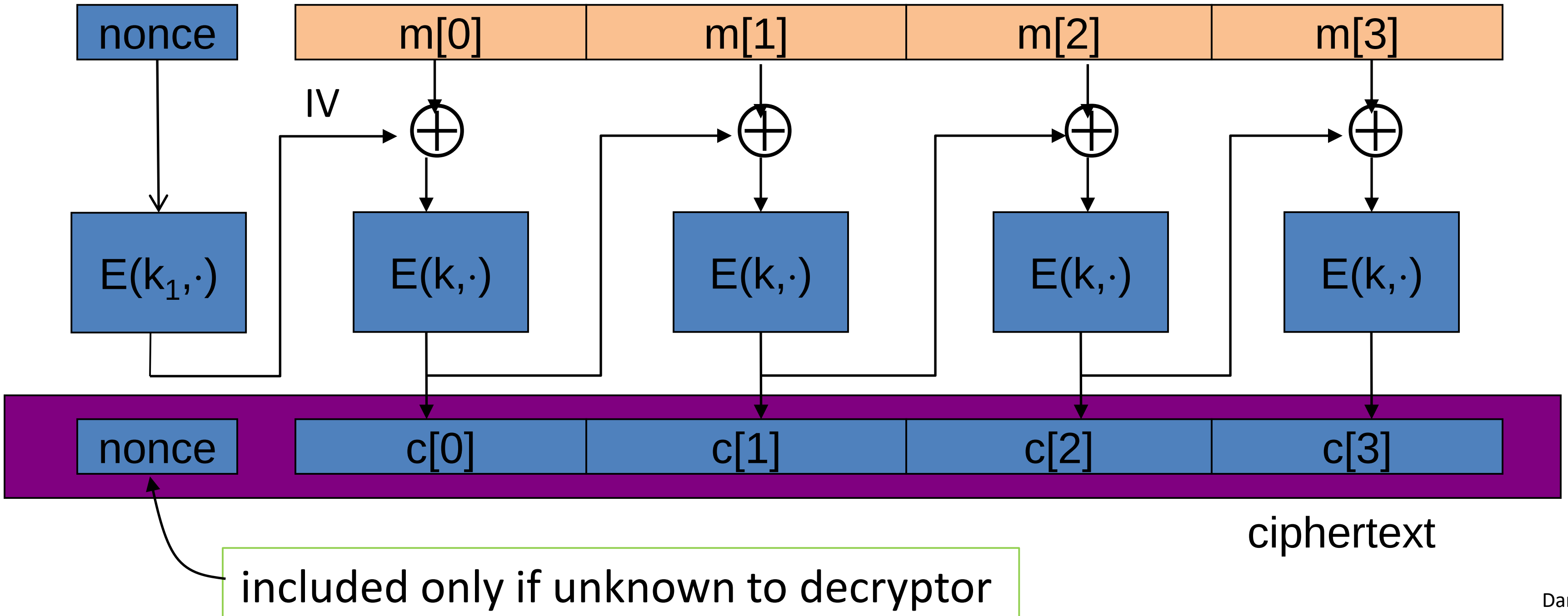


Bug in SSL/TLS 1.0: IV for record #i is last CT block of record #(i-1)

Construction 1': nonce-based CBC

- Cipher block chaining with <u>unique</u> nonce: key = (k,k_1)

unique nonce means: (key, n) pair is used for only one message



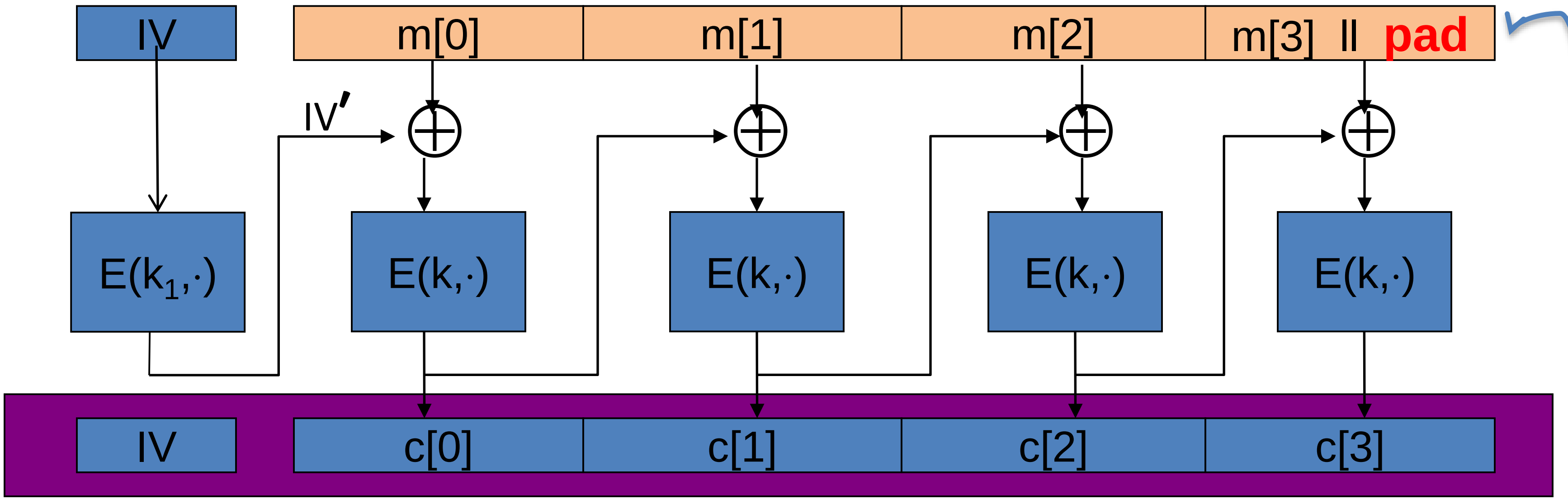
An example Crypto API (OpenSSL)

```
void AES_cbc_encrypt(
        const unsigned char *in,
        unsigned char *out,
        size_t length,
        const AES_KEY *key,
        unsigned char *ivec,          ⟵ user supplies IV
        AES_ENCRYPT or AES_DECRYPT);
```

otherwise, no CPA security

When nonce is non random need to encrypt it before use

A CBC technicality: padding



removed during decryption

TLS: for n>0, n byte pad is | n | n | n | ••• | n |

if no pad needed, add a dummy block

End of Segment

Using block ciphers

Modes of operation: many time key (CTR)

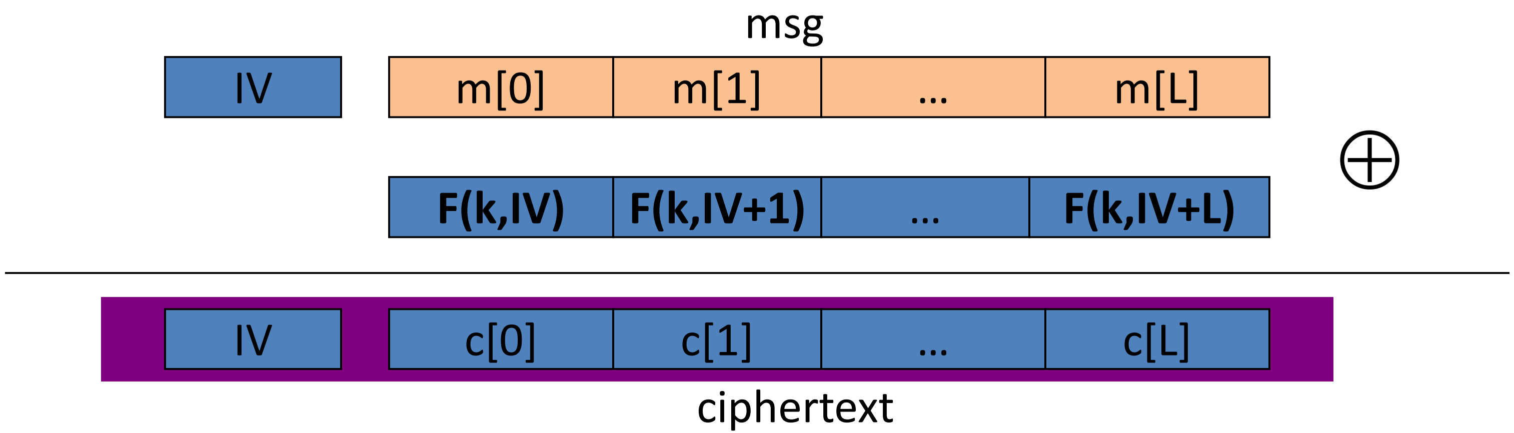
<u>Example applications</u>:

1. File systems: Same AES key used to encrypt many files.
2. IPsec: Same AES key used to encrypt many packets.

Construction 2: rand ctr-mode

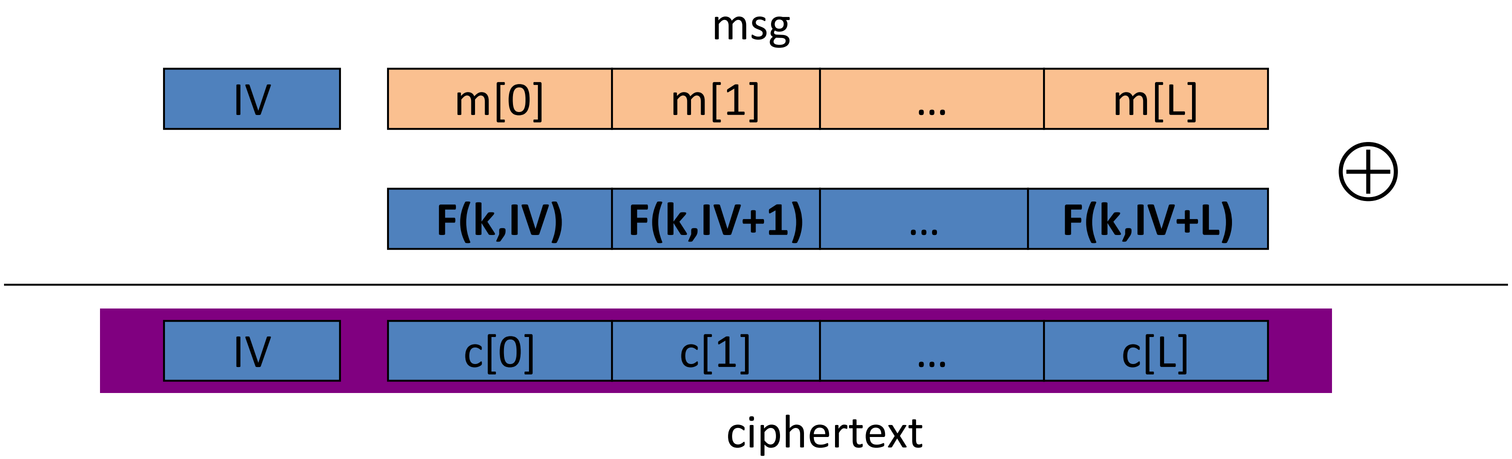
Let $F: K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a secure PRF.

$E(k,m)$: choose a random $IV \in \{0,1\}^n$ and do:

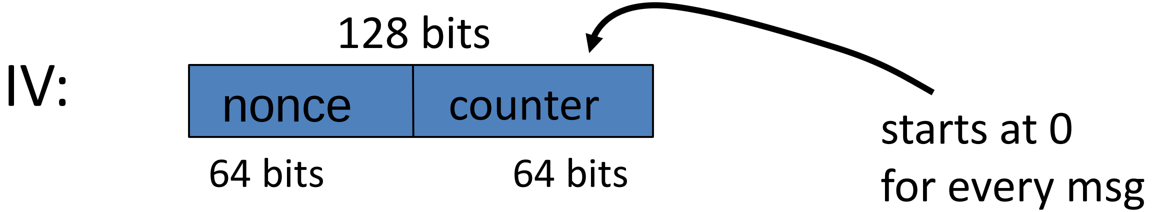


note: parallelizable (unlike CBC)

Construction 2': nonce ctr-mode



To ensure F(k,x) is never used more than once, choose IV as:



rand ctr-mode (rand. IV): CPA analysis

- Counter-mode Theorem: For any L>0,

  If F is a secure PRF over (K,X,X) then

  E_{CTR} is a sem. sec. under CPA over (K, X^L, X^{L+1}).

  In particular, for a q-query adversary A attacking E_{CTR}

  there exists a PRF adversary B s.t.:

$$Adv_{CPA}[A, E_{CTR}] \leq 2 \cdot Adv_{PRF}[B, F] + \mathbf{2\, q^2\, L / |X|}$$

Note: ctr-mode only secure as long as $q^2 L << |X|$. Better than CBC !

An example

$$\text{Adv}_{\text{CPA}}[A, E_{\text{CTR}}] \leq 2 \cdot \text{Adv}_{\text{PRF}}[B, E] + \mathbf{2\, q^2\, L\, /\, |X|}$$

q = # messages encrypted with k , L = length of max message

Suppose we want $\text{Adv}_{\text{CPA}}[A, E_{\text{CTR}}] \leq 1/2^{32}$ $\Leftarrow$ $q^2 L / |X| < 1/2^{32}$

- AES: $|X| = 2^{128}$ $\Rightarrow$ $q\, L^{1/2} < 2^{48}$

So, after 2^{32} CTs each of len 2^{32}, must change key

(total of 2^{64} AES blocks)

Comparison: ctr vs. CBC

	CBC	ctr mode
uses	PRP	PRF
parallel processing	No	Yes
Security of rand. enc.	$q^2 L^2 \ll \|X\|$	$q^2 L \ll \|X\|$
dummy padding block	Yes	No
1 byte msgs (nonce-based)	16x expansion	no expansion

(for CBC, dummy padding block can be solved using ciphertext stealing)

Summary

- PRPs and PRFs: a useful abstraction of block ciphers.

- We examined two security notions: (security against eavesdropping)
  1. Semantic security against one-time CPA.
  2. Semantic security against many-time CPA.

  Note: neither mode ensures data integrity.

- Stated security results summarized in the following table:

Goal \ Power	**one-time key**	**Many-time key (CPA)**	**CPA and integrity**
Sem. Sec.	steam-ciphers det. ctr-mode	rand CBC rand ctr-mode	later

Further reading

- A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation, M. Bellare, A. Desai, E. Jokipii and P. Rogaway, FOCS 1997

- Nonce-Based Symmetric Encryption, P. Rogaway, FSE 2004

End of Segment