Using block ciphers

Modes of operation: many time key (CTR)

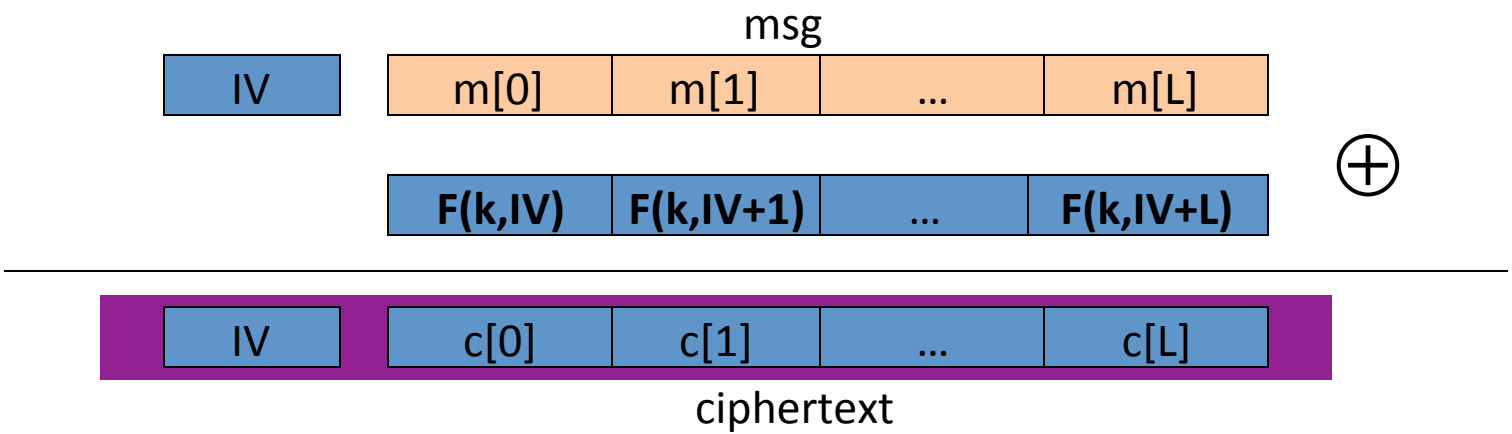
Example applications:

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

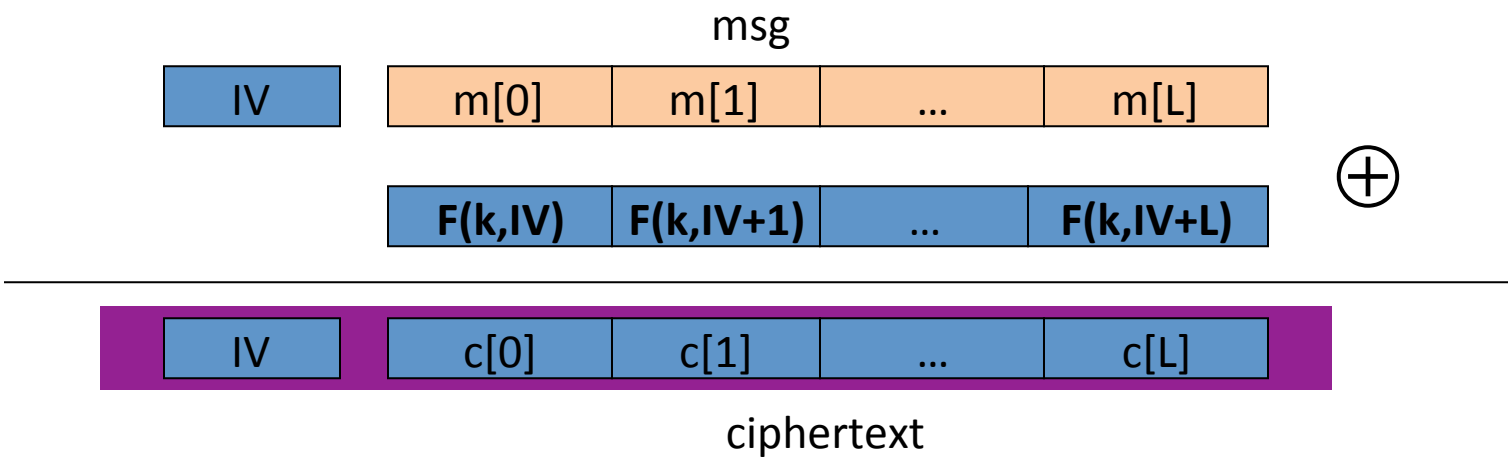
Let $F: K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a secure PRF.

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

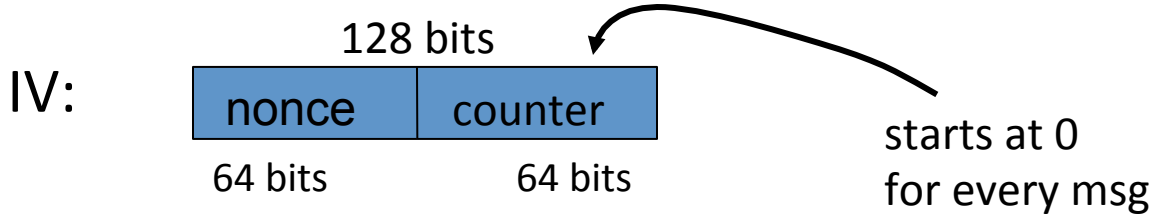


note: parallelizable (unlike CBC)

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.:

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

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

An example

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

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

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

- 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.	$q^2 L^2 << \|X\|$	$q^2 L << \|X\|$
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