Today in Cryptography (5830)

DES, AES
Feistel constructions
Length-preserving encryption
Length-extending encryption

Block ciphers

- Family of permutations, one permutation for each key

$$E : \{0,1\}^k \times \{0,1\}^n \dashrightarrow \{0,1\}^n$$

$$E(K,X) = Y \qquad\qquad D(K,Y) = X$$

Ideal block cipher & CTR mode

- Imagine everyone has access to an idealized version of block cipher: random look-up table
- We saw how to build CTR-mode encryption last time using an ideal cipher

Enc(K,M):
IV <-\$ $\{0,1\}^n$
Parse M into $M_1,\ldots,M_m$
For i = 1 to m do
    C_i <- E(K,IV + i) + M_i
Ret IV || C_1 || … || C_m

Where X + Y is bitwise XOR of first b bits of X and Y for b = min {|X|,|Y|}

|| means bit string concatenation

- Secure if |K| >> adversary runtime & $2^n \gg q^2$

How do we build efficient block ciphers that are close to ideal?

$E : \{0,1\}^k \times \{0,1\}^n \dashrightarrow \{0,1\}^n$

$E(K,X) = Y$ $\qquad\qquad$ $D(K,Y) = X$

Advanced Encryption Standard (AES)

Rijndael (Rijmen and Daemen)

n = 128
k = 128, 192, 256

Number of keys for k=128:
340,282,366,920,938,463,463,374,607,431,768,211,456

Substitution-permutation design.
For k=128 uses 10 rounds of:

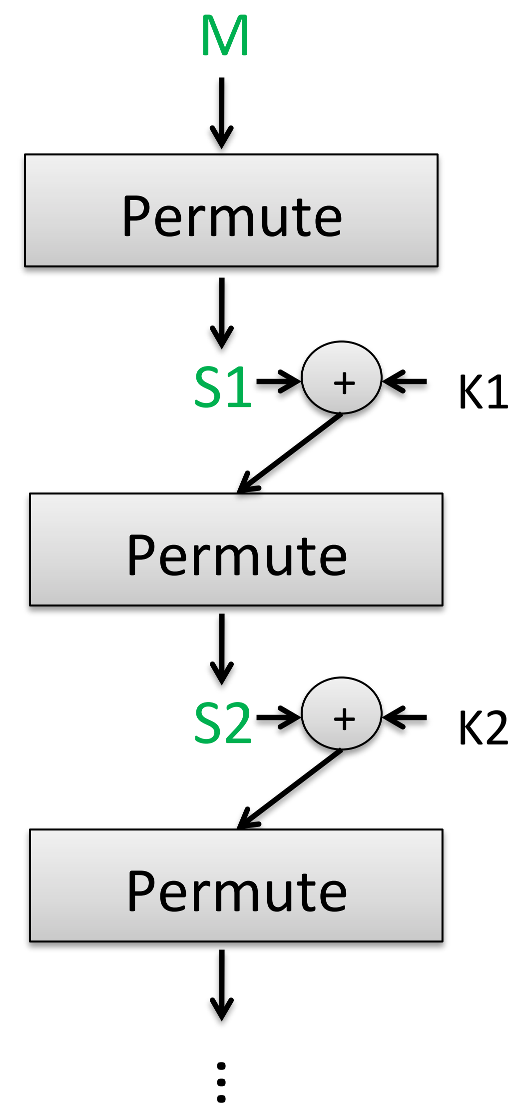
1) Permute:

SubBytes (non-linear S-boxes)

ShiftRows + MixCols (invertible linear transform)

2) XOR in a round key derived from K

(Actually last round skips MixCols)



Best attacks against AES

Brute-force attack (try all keys): worst case time about 2^{128}

Attack	Attack type	Complexity	Year
Bogdanov, Khovratovich, Rechberger	chosen ciphertext, recovers key	$2^{126.1}$ time + some data overheads	2011

No direct attacks of practical interest known

Side-channel attacks do exist, need to implement carefully

Data encryption standard (DES)

Originally called Lucifer
- team at IBM
- input from NSA
- standardized by NIST in 1976

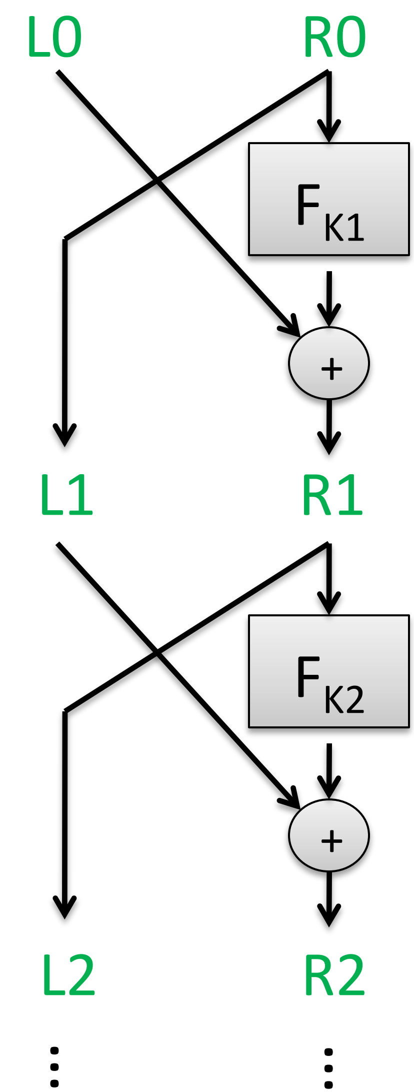
$n = 64$
$k = 56$

Number of keys:
72,057,594,037,927,936

Split 64-bit input into L0,R0 of 32 bits each

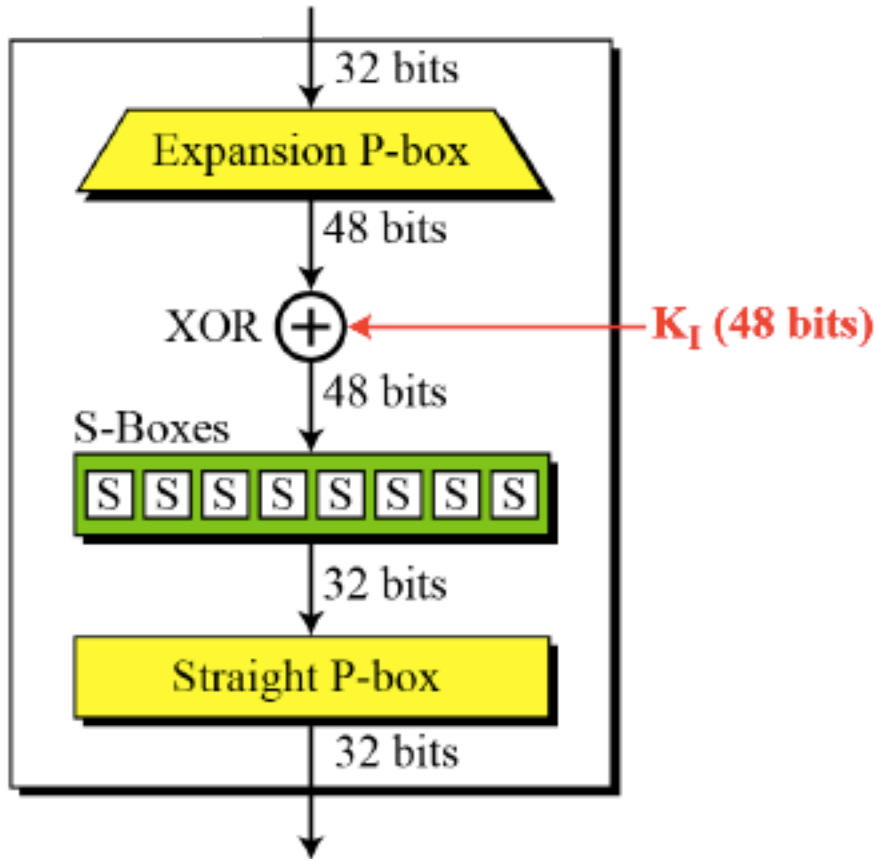
Repeat Feistel round 16 times

Each round applies function F using separate round key



Round functions in DES

X



$F(K_i, X)$

Best attacks against DES

Attack	Attack type	Complexity	Year
Biham, Shamir	Chosen plaintexts, recovers key	2^{47} plaintext, ciphertext pairs	1992
DESCHALL	Brute-force attack	$2^{56}/4$ DES computations 41 days	1997
EFF Deepcrack	Brute-force attack	~4.5 days	1998
Deepcrack + DESCHALL	Brute-force attack	22 hours	1999

- DES is still used in some places
- 3DES (use DES 3 times in a row with more keys) expands keyspace and still used widely in practice

The History

- DES (under name Lucifer) designed by IBM in 1970s
- NIST standardized it
  - NSA evaluated it and made suggested changes to shorten key length to 56 bits and changes to S-boxes
  - Many public criticisms of these changes, though S-boxes change actually strengthened DES
- AES competition run by NIST (1997-2000)
  - Many good submissions (15 total submissions)
  - AES chosen as winner

Applications of block ciphers (sometimes called modes of operation)

We'll look closely at two encryption applications:

- **Length-preserving encryption**
  - Useful for cases where ciphertexts must be same length as plaintexts.
  - Should only be used when absolutely needed
- **Length-extending encryption**
  - Insecure variants: CTR mode, ECB mode, CBC mode
  - We'll build secure ones in a few lectures

Example: Credit card number encryption

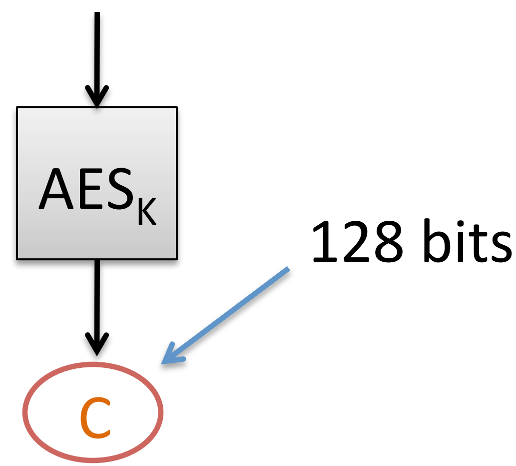
Jane Doe	1343-1321-1231-2310
Thomas Ristenpart	9541-3156-1320-2139
John Jones	5616-2341-2341-1210
Eve Judas	2321-4232-1340-1410

Database schemas and software require <= 16 decimal digits and valid Luhn checksum

$$AES_K : \{0,1\}^{128} \longrightarrow \{0,1\}^{128}$$

Ciphertexts are too big for replacing plaintext within database!

M = 2321-4232-1345-1415



Example: Credit card number encryption

Jane Doe	
Thomas Ristenpart	
John Jones	
Eve Judas	

Database schemas and software require <= 16 decimal digits and valid Luhn checksum

Encryption tool whose ciphertexts are also credit-card numbers

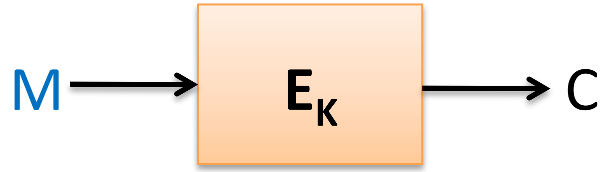
$$E_K : [0..9]^{16} \longrightarrow [0..9]^{16}$$

Valid credit-card number

$\mathbf{E}_K$

Valid credit-card number

Format-preserving encryption (FPE)



Enjoys format N

Enjoys format N

Disk sectors / payment card numbers just two examples
Some others:

1) Valid addresses for a certain country

2) 4096-byte disk sectors

3) Assigned Social Security Numbers (9 digits, without leading 8 or 9)

4) Composition of (1) and (3)

How to build FPE on 40 bits?

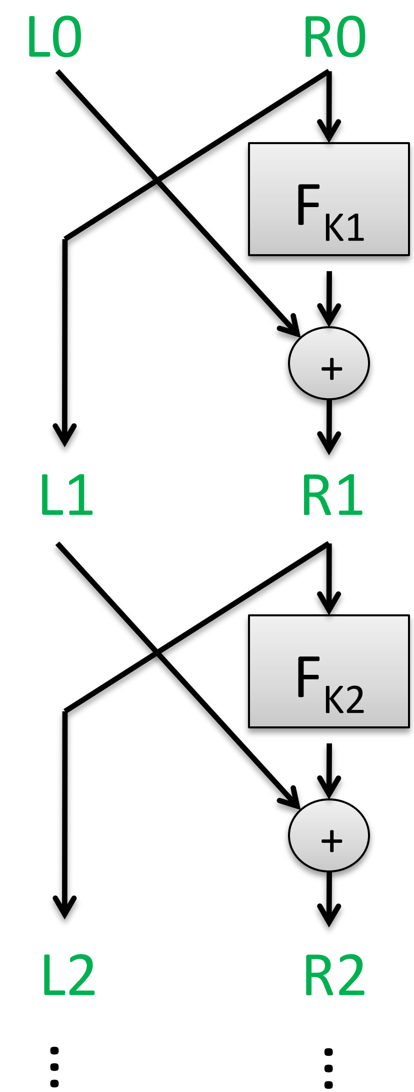
Special case of FFX encryption

Input M = 40 bits
L0 = 20 bits
R0 = 20 bits

$F_{K1}(R) = AES(K, 1 \; || \; R)$
$F_{K2}(R) = AES(K, 2 \; || \; R)$
…

Take XOR mod 2^{20}

Use 10 rounds

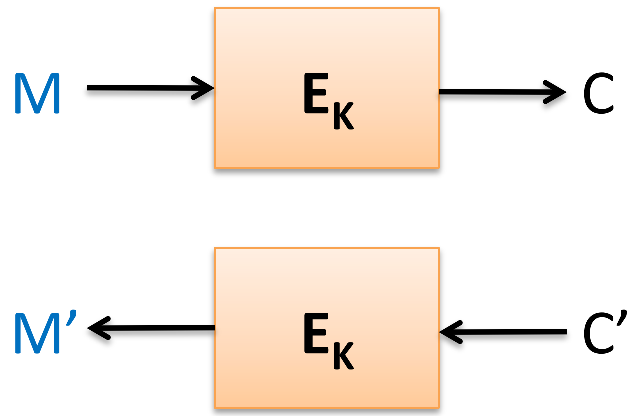


Balanced Feistel security in theory

- Luby & Rackoff showed that if round functions are random and n is relatively large, then
  - 3 rounds suffice for chosen-plaintext attack security in sense of pseudorandom permutation
  - 4 rounds suffice for chosen-ciphertext attack security pseudorandom permutation
  - Proofs hold up to $q \approx 2^{n/4}$

- Sometimes n is not very large:
  - FFX designers suggested 10 rounds as heuristic

Security problems with length-preserving encryption?



Looks like a random string (subject to permutivity)

Looks like a random string (subject to permutivity)

Any C' ≠ C

But determinism has problems:

	Plaintext	Ciphertext
Jane Doe	1343-1321-1231-2310	1049-9310-3210-4732
Thomas Ristenpart	9541-3156-1320-2139	7180-4315-4839-0142
John Jones	2321-4232-1340-1410	5731-8943-1483-9015
Eve Judas	1343-1321-1231-2310	1049-9310-3210-4732

Applications of block ciphers (sometimes called modes of operation)

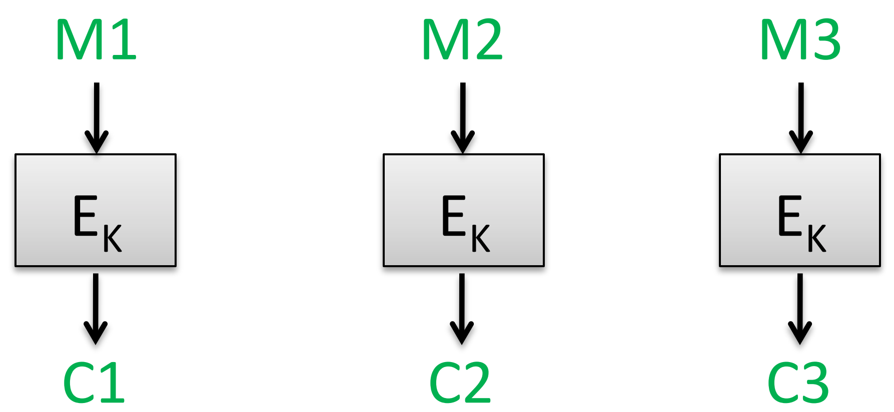
We'll look closely at two encryption applications:

- Length-preserving encryption
  - Useful for cases where ciphertexts must be same length as plaintexts.
  - Should only be used when absolutely needed
- Length-extending encryption
  - Insecure variants: CTR mode, ECB mode, CBC mode
  - We'll build secure ones in a few lectures

Block cipher modes of operation

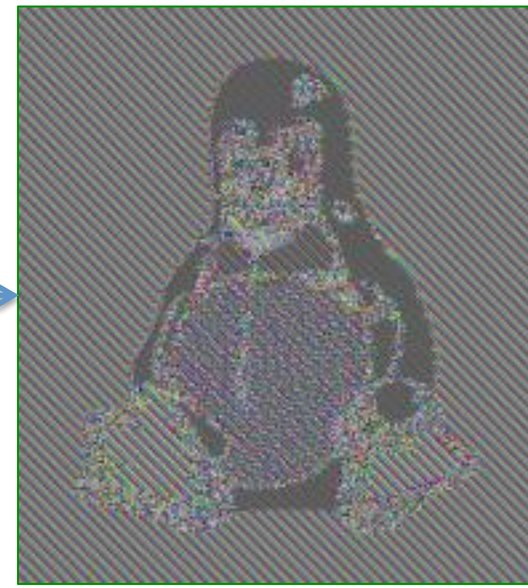
How can we build an encryption scheme for arbitrary message spaces out of a block cipher?

Electronic codebook (ECB) mode
Pad message M to M1,M2,M3,... where each block Mi is n bits
Then:



ECB mode is a more complicated looking substitution cipher

Encrypted with ECB



Images courtesy of
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

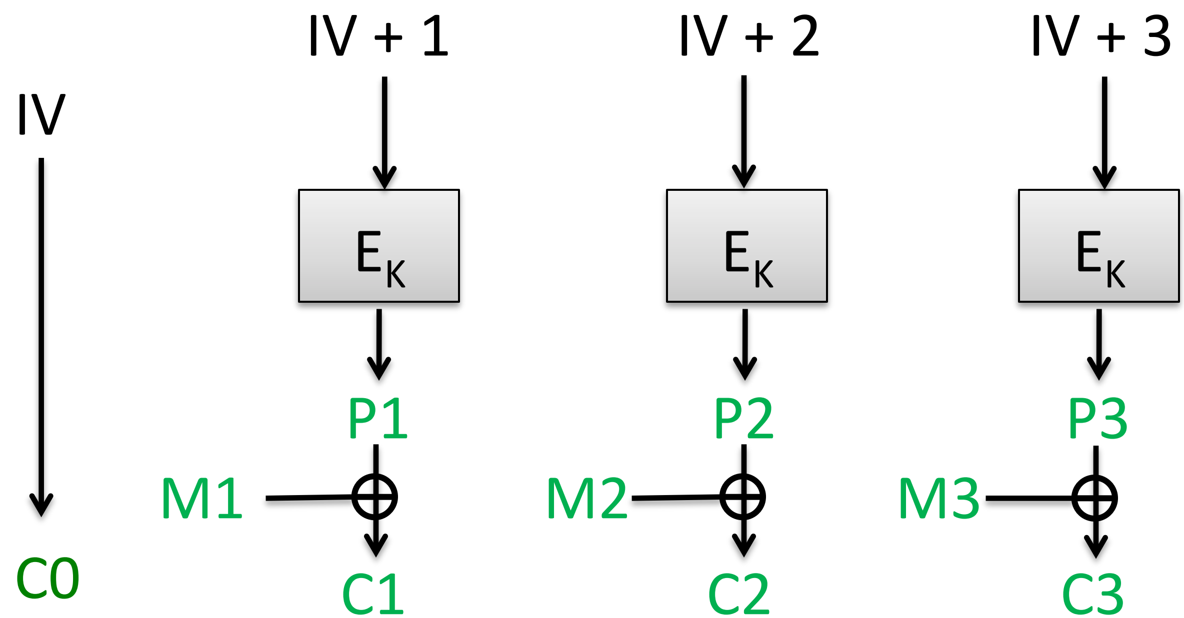
CTR mode encryption using block cipher

Counter mode (CTR)

Pad message M to M1,M2,M3,... where each is n bits except last

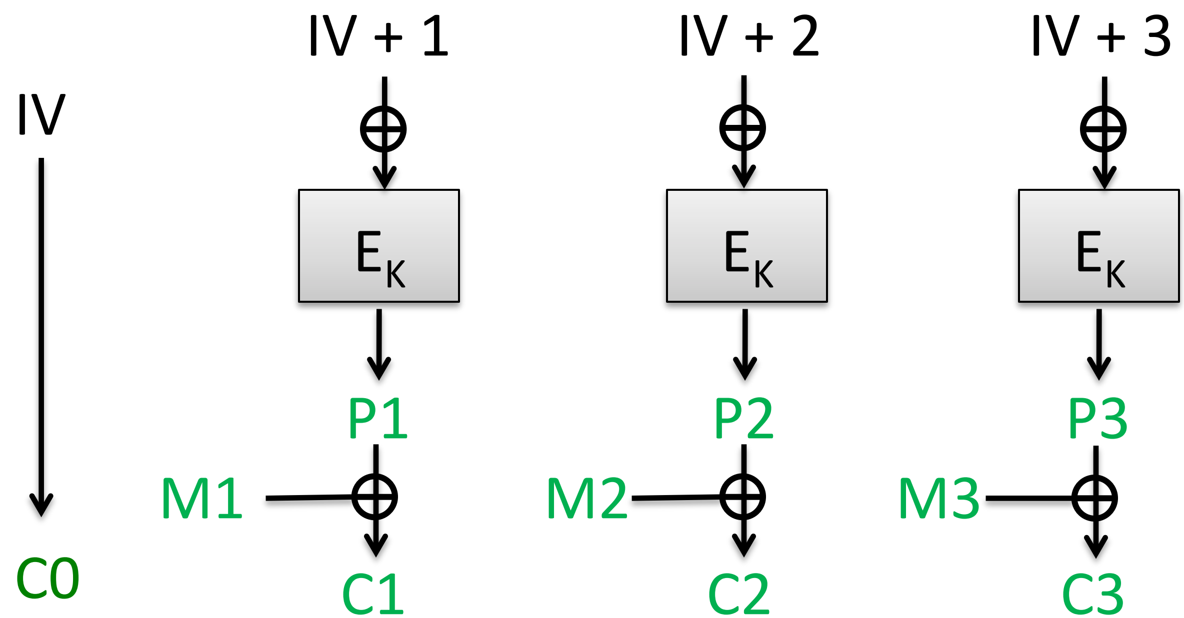
Choose random n-bit string IV

Then:



Maybe use less than full n bits of P3

How do we decrypt?



Can attacker learn K from just C0,C1,C2,C3?

Implies attacker can break E, i.e. recover block cipher key

Can attacker learn M = M1,M2,M3 from C0,C1,C2,C3?

Implies attacker can invert the block cipher without knowing K

Can attacker learn one bit of M from C0,C1,C2,C3?

Implies attacker can break PRF security of E

Passive adversaries cannot learn anything about messages

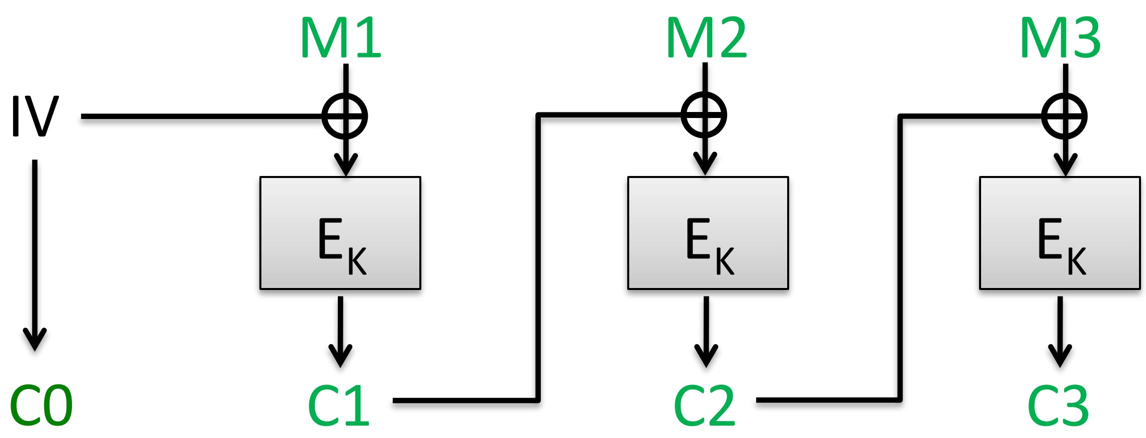
CBC mode

Ciphertext block chaining (CBC)

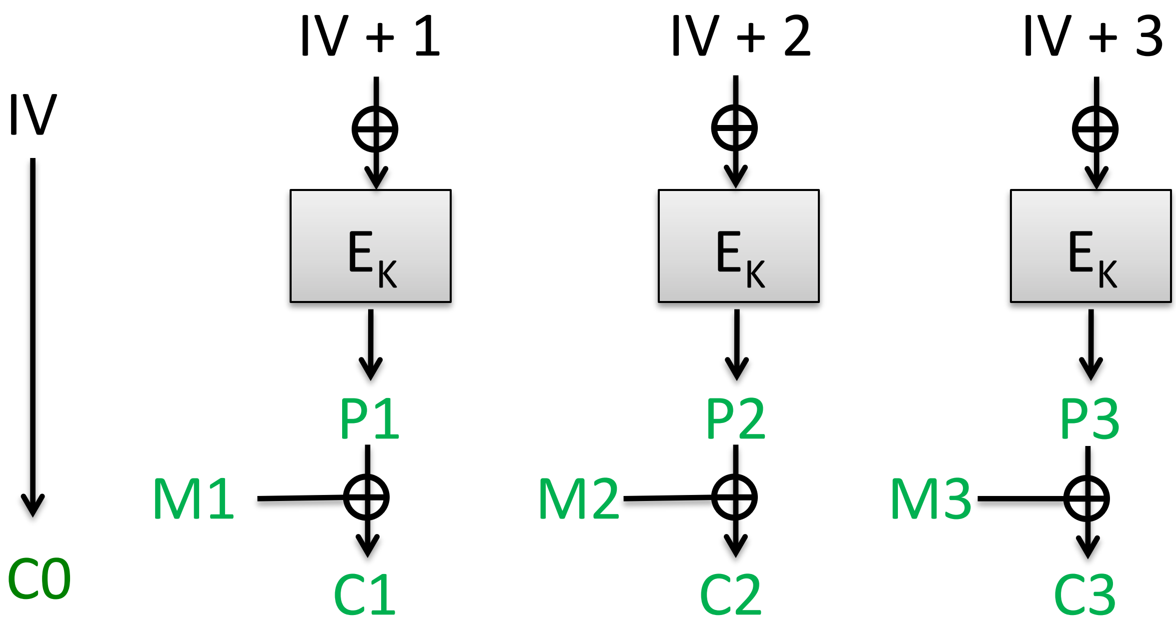
Pad message M to M1,M2,M3,... where each block Mi is n bits

Choose random n-bit string IV

Then:



How do we decrypt?



<u>Theorem (informal).</u>
Let A be a successful, efficient attacker against security of CBC mode. Then there exists a PRF adversary B against E that is efficient and successful.

<u>Security proofs (reductions)</u>

Breaking scheme

Breaking assumptions

Attacker can break CBC confidentiality

Attacker can not break CBC confidentiality

Can break E in PRF sense

Can not break E in PRF sense

Reduces analysis now to E and to security definition / model

None of these modes are secure for encryption

- ECB is obviously insecure
- CTR mode and CBC mode fail in presence of active attacks
  - Cookie example
  - Adversaries are unlikely to ever be fully passive
- More on this next lecture