6.857 Computer and Network Security
Lecture 9

Project Idea:
- Security of automotive info systems

Misc:
- TLS bugs (Apple, not Linux)

Today: Block Ciphers
- Modes of operation: ECB, CTR, CBC, CFB
- IND-CCA security definition
- UFE mode
- Start MACs (if time)

For practical purposes, can treat AES as ideal block cipher:

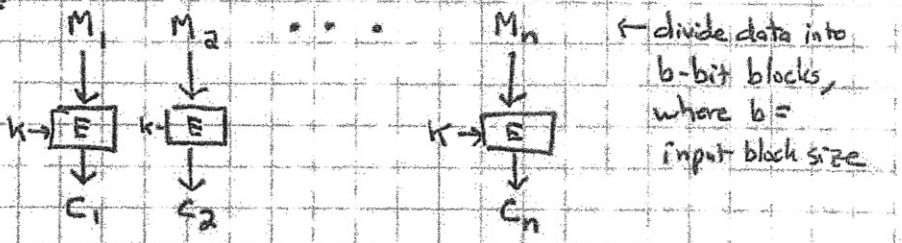
[For each key, mapping $Enc(K, \cdot)$ is a random independent permutation of $\{0,1\}^{128}$ to itself.

Modes of Operation:

How to encrypt variable-length messages? (using AES)

"ECB" = "Electronic code book"
"CTR" = "Counter mode"
"CBC" = "Cipher-block chaining" (& CBC-MAC)
"CFB" = "Cipher feedback"
... (others...)

ECB:



To handle data that is not a multiple of b bits in length:
- Append a "1" bit (always)
- Append enough "0" bits to make length a multiple of b bits.

This gives invertible (1-1) "padding" operation.
Pad before encryption; unpad after decryption.

ECB preserves many patterns: repeated message blocks
⇒ repeated ciphertext blocks

ECB really only good for encrypting random data (e.g. keys)

TOPIC:

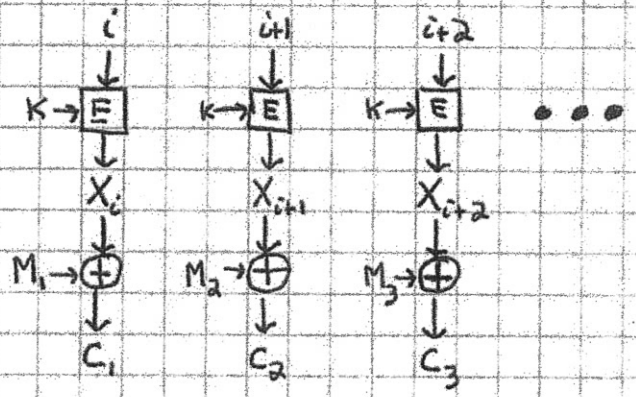
DATE:

FILE UNDER:

PAGE: L5.6.

CTR (Counter mode):

Generate a PR (pseudorandom) sequence by encrypting $i, i+1, \ldots$
XOR with message to obtain ciphertext.



Initial counter value can be transmitted first:

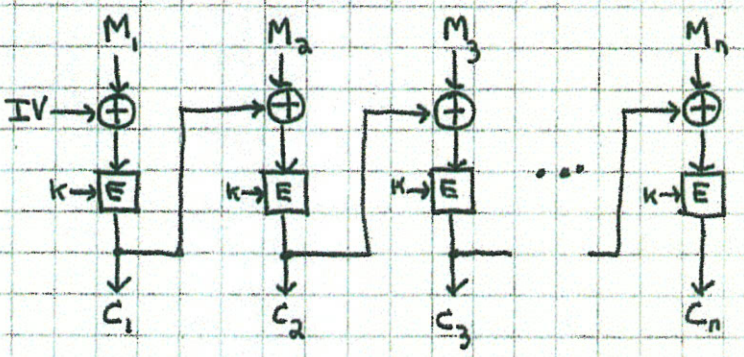
$i, C_1, C_2, \ldots$

Of course, no counter value should be re-used!

CBC (Cipher-block chaining):

Choose IV ("initialization value") randomly, then use each C_i as "IV" for M_{i+1}. Transmit IV with ciphertext:

$$IV, C_1, C_2, \ldots, C_n$$



Decryption easy, and parallelizable (∴ little error propagation)

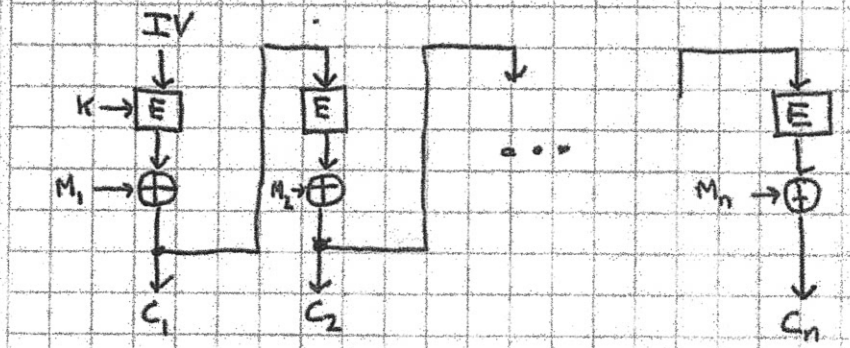
Lookup "ciphertext stealing" for cute way of handling messages that are not a multiple of b bits in length. This method give ciphertext length = message length.

fixed IV is usually all 0's →

Last block C_n is the "CBC-MAC" (CBC Message Authentication code) for message M. [A fixed IV is used here.] The MAC is a "cryptographic checksum" (more later...) (If messages have variable length then key for last block should be different.)

CFB (Cipher feedback mode)

Similar to CBC mode. Uses random IV transmitted with ciphertext.



If M is not a multiple of b bits in length, can just transmit shortened ciphertext. (No need for ciphertext stealing.)

Are these modes good ones? What do we want?

Goal → If block cipher is indistinguishable from ideal block cipher then mode provides indistinguishability based on chosen ciphertext attack (IND-CCA):

- Define as game with adversary.
- Mode is IND-CCA secure if adversary can win with probability at most $\frac{1}{2} + \varepsilon$ for "negligible" ε.

Let K be randomly chosen key.
Let E_K denote encryption (using mode) with key K.
Let D_K denote decryption

Phase I ("Find"):

- Adversary given black-box access to E_K, D_K (can encrypt/decrypt whatever it likes)
- Adversary outputs two messages m_0, m_1, of same length, plus state information s.

Phase II ("Guess"):

- Examiner secretly picks $d \xleftarrow{R} \{0,1\}$
  Examiner computes $y = E_K(m_d)$
- Adversary given y, s, access to E_K, and access to D_K (except on y)
- Adversary computes for a while, then must produce bit $\hat{d}$ as its guess for d.
- Adversary's advantage is $\left| P(\hat{d}=d) - \frac{1}{2} \right|$.

Encryption secure against CCA attack if advantage is negligible.

Theorem: Modes ECB, CTR, CBC, CFB are not IND-CCA secure.

Proof: Adversary picks $m_0 = 0^x$, $m_1 = 1^x$ for large x.

Then $y = E_k(m_d)$

Let $z = 1^{st}$ half of y.

Since $z \neq y$, Adversary allowed in phase II to ask for $D_k(z)$.

This gives first half of m_d, revealing d.

Adversary always wins. ▨

Can one design a IND-CCA scheme?

Given a ciphertext y for a message m,

Adversary should not be able to construct a

ciphertext z for a related (e.g. truncated) message.

(nonmalleability)

TOPIC:

DATE:

FILE UNDER:

PAGE:

Fact:

To be IND-CCA secure,

encryption method must be randomized or stateful!

(else Adv can encrypt m_0 & m_1 during Phase I,

and compare to y in Phase II.)

(Randomization used should be unknown to Adv, too.)

(If state is used, encryption method can use pseudo-random values rather than random values, e.g. have another key K' and a counter i, and generate pseudo random values from K' and i to use instead of the truly random values.)

Here is a sketch of one IND-CCA secure method.
(due to Desai. UFE = "Unbalanced Feistel encryption")

M = long message, sequence $M_1, M_2, \ldots, M_n$ of b-bit blocks.

$K = (K_1, K_2, K_3)$ Three indep. keys for block ciphers

$r \xleftarrow{R} \{0,1\}^b$ starting counter value

pad $P = P_1, P_2, \ldots, P_n$ where $P_i = E_{K_1}(r+i)$ ← (CTR mode)

ciphertext $C = C_1, C_2, \ldots, C_n$ where $C_i = M_i \oplus P_i$

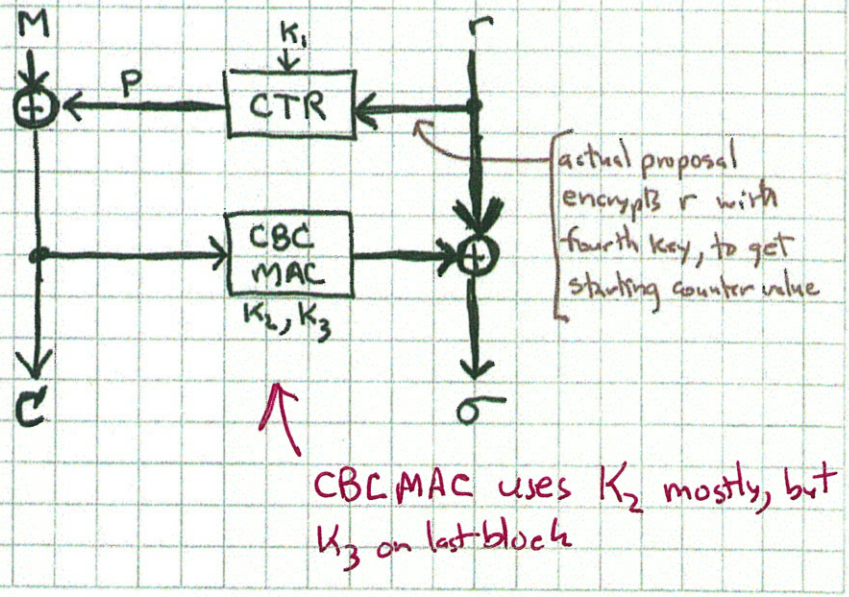
CBC-MAC: $X_0 = 0^b$

$X_i = E_{K_2}(X_{i-1} \oplus C_i) \quad 1 \le i < n$

$X_n = E_{K_3}(X_{n-1} \oplus C_n)$ (MAC)

$\sigma = r \oplus X_n$ use MAC to mask r
(no message authentication)

Output: $C_1, C_2, \ldots, C_n, \sigma$



- Encryption with UFE can be done in single pass over data, but decryption requires two passes: ("online" property)
  - first to compute mac X_n, then to get r
  - second to decrypt C to get M
- Only designed for <u>confidentiality</u> (there is no way provided for receiver to tell if ciphertext has been tampered with.) (Need to use MAC on top of all of this, or some "combined mode" providing <u>both</u> confidentiality & integrity.)
- Note "unbalanced Feistel structure".
- Length of ciphertext $(C, \sigma) = |M| + |r|$;
  expansion only as needed for randomization.
  No need for "ciphertext stealing" since we use CTR mode.

6.857 Network and Computer Security

Spring 2014