TOPIC: 6.857 - Computer & Network Security

DATE: 3/6/13

FILE UNDER:

PAGE: L09.1

Admin:

No project idea presentations in class Monday...
(use Piazza & recitation instead...)

Today:

Modes of operation for block ciphers (cont'd)

- ☐ CBC (Cipher block chaining)
- ☐ CFB (Cipher feedback mode)
  - IND-CCA security defn
- ☐ UFE (Unbalanced Feistel mode)

↓

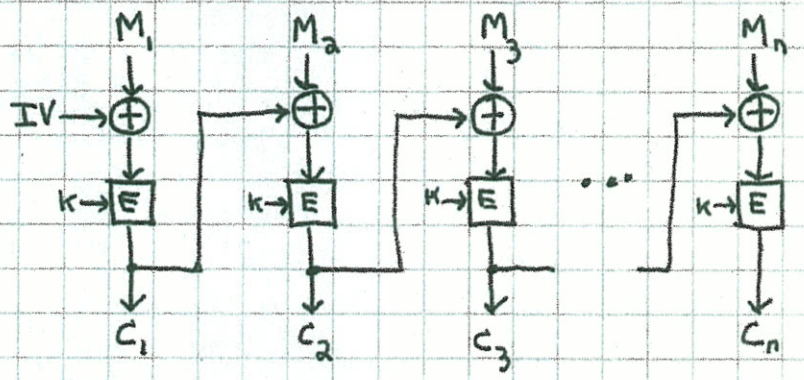
Message Authentication Codes (MAC's) (defn)

- ☐ HMAC, CBC-MAC, PRF-MAC
- ☐ One-time MAC (problem stmt)

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)

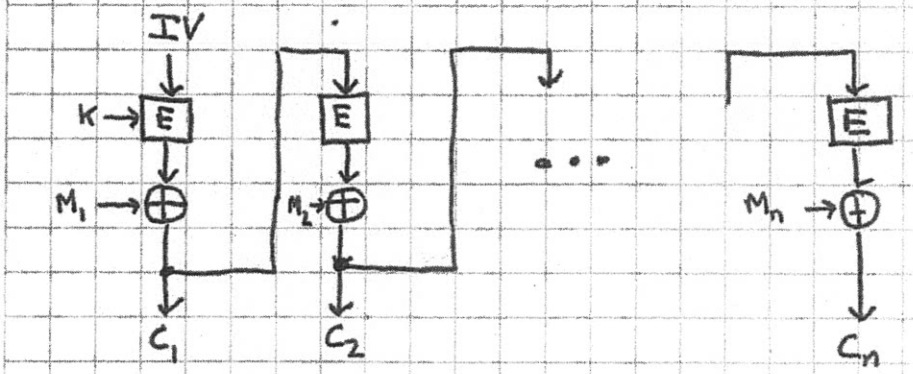
Lookup "ciphertext stealing" for cute way of handling messages that are not a multiple of b bits in length. This method give ciphertext length = message length.

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 $1/2 + \epsilon$ 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 $|P(\hat{d}=d) - 1/2|$.

Encryption secure against CCA attack if advantage is negligible.

TOPIC:

DATE:

FILE UNDER:

PAGE:

Fact: To be IND-CCA secure,

encryption method must be randomized!

(else Adv can encrypt m_0, m_1 & compare to y)

(Also: random values used should not be evident/available to Adv, so Adv can use them in decryption.)

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 = 1st 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)

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 $C_i = M_i \oplus P_i$

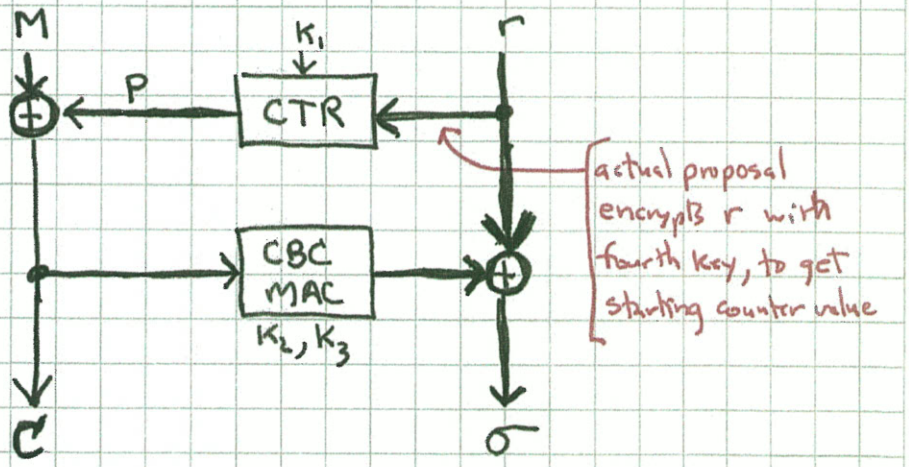
CBC-MAC: $X_0 = 0^b$

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

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

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

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

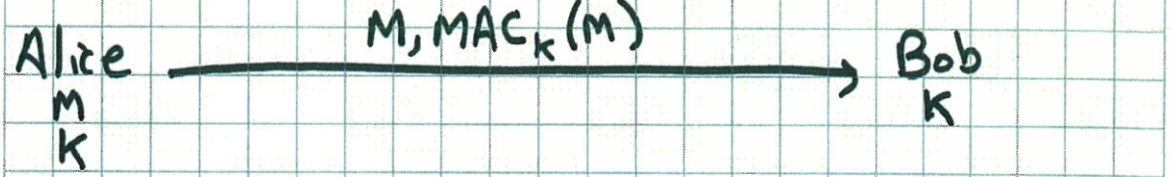


("online" property)

- Encryption with UFE can be done in single pass over data, but decryption requires two passes:
  - first to compute mask 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.

MAC (Message Authentication Code)

- Not confidentiality, but integrity (recall "CIA")
- Alice wants to send messages to Bob, such that Bob can verify that messages originated with Alice & arrive unmodified.
- Alice & Bob share a secret key K
- Orthogonal to confidentiality; typically do both (e.g. encrypt, then append MAC for integrity)
- Need additional methods (e.g. counters) to protect against replay attacks



[Here M is message to be authenticated, which could be ciphertext resulting from encryption.]

- Alice computes $MAC_K(M)$ & appends it to M.
- Bob recomputes $MAC_K(M)$ & verifies it agrees which what is received. If ≠, reject message.

Note if MAC has t bits, then Adv can forge with prob 2^{-t}, just by guessing. t=32 might be ok in practice...

Adversary (Eve) wants to forge $M', MAC_K(M')$ pair that Bob accepts, without Eve knowing K.

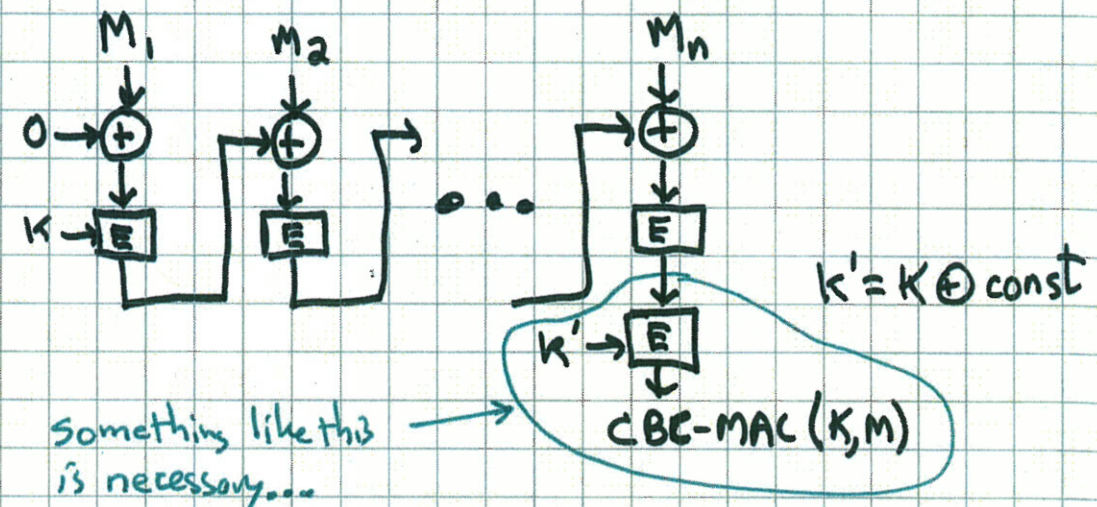
- She may hear a number of valid $(M, MAC_K(M))$ pairs first, possibly even with M's of her choice (chosen msg attacks).
- She wants to forge for M' for which she hasn't seen $(M', MAC_K(M'))$ valid pair.

Two common methods:

$HMAC(K,M) = h(K_1 \| h(K_2 \| M))$

where $K_1 = K \oplus opad$, $K_2 = K \oplus ipad$ { opad, ipad are fixed constants

$CBC\text{-}MAC(K,M) \cong$ last block of CBC enc. of M



MAC using random oracle (PRF):

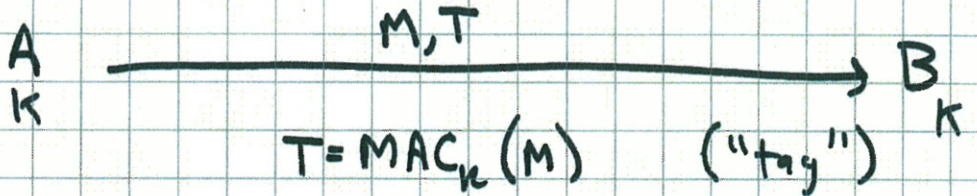
$$MAC_K(M) = h(K \| M)$$

(OK if h is indistinguishable from RO, which means, as we saw, for sequential hash fns, that last block may need special treatment.)

One-Time MAC (problem stmt):

Can we achieve security against unbounded Eve, as we did for confidentiality with OTP, except here for integrity?

Here key K may be "use-once" [as it was for OTP].



- Eve can learn M, T then try to replace M, T with M', T' (where M' ≠ M) that Bob accepts.
- Eve is computationally unbounded.

	Confidentiality	Integrity
Unconditional	OTP ✓	One-time MAC?
Conventional (symmetric key)	Block ciphers (AES) ✓	MAC (HMAC) ✓
Public-key (asymmetric)	PK enc.	Digital signature