Admin: Pset #2 due March 11.

Today: Symmetric Encryption
Authentication

Recall: Block ciphers

Encrypts blocks of fixed length

$$m \downarrow \boxed{E_k} \downarrow c$$

"Ideal cipher": Random permutation

Eg. of block ciphers: DES & AES

Note: Even an "ideal cipher" does not offer "perfect security".
Eg. the adv can see if the same msg is encrypted twice

Main Drawback: Encrypts msgs of fixed length

Symmetric Encryption:

Allows to encrypt msgs of arbitrary length

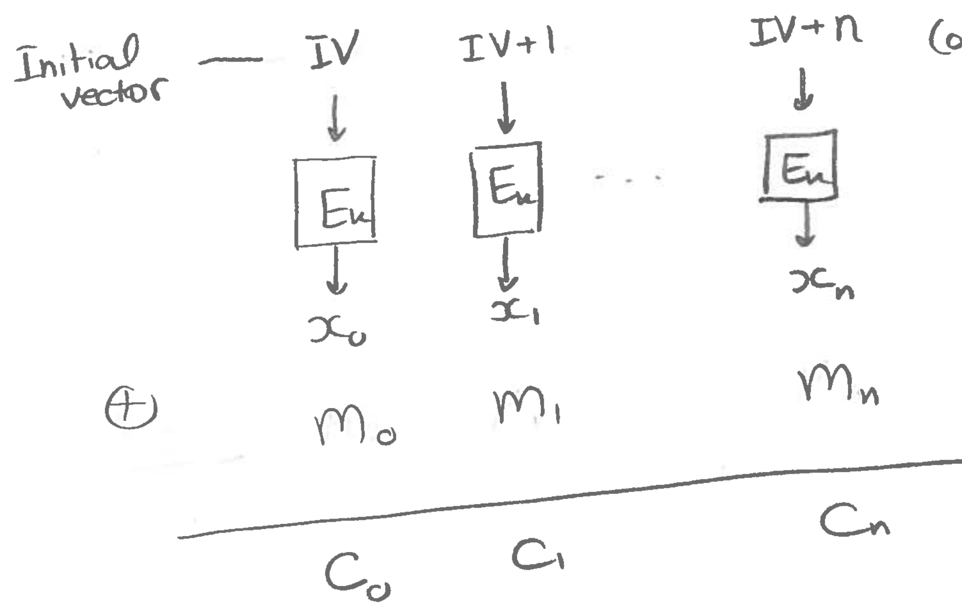
Electronic Codebook → ECB Mode

Mode of Operation Uses a block cipher to obtain a symmetric encryption.

Insecure attempt: $M = (m_0, m_1, \ldots m_n)$ $\quad c_i = E_k(m_i)$ output $(c_0, c_1, \ldots c_n)$.

Counter mode (CTR) : Generates pseudorandom bits from the key, and encrypts msg by xoring w. pseudorandom bits (a la one time pad)

known as a stream cipher

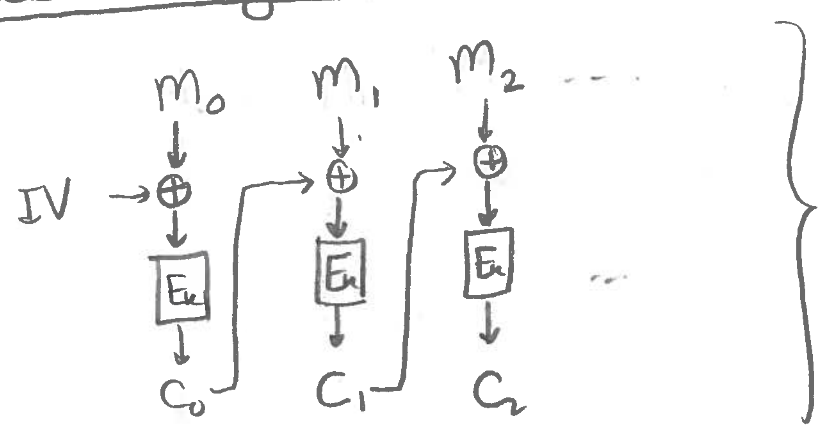


output IV, $(c_0, c_1, \ldots, c_n)$

Should never use same IV twice!

(for example, can choose IV at random).

Cipher Block Chaining Mode (CBC)



output IV, $(c_0, c_1, \ldots)$

* In CBC mode, if msg is not of length which is a multiple of block length, need to pad. (eg. add 10...0 to each msg)

Are these modes of operations secure?

We consider two security notions:

Security against Chosen Plaintext Attacks (CPA)

Security against Chosen Ciphertext Attacks (CCA).

Claim: If block cipher is indistinguishable from ideal cipher then these encryption schemes are CPA secure (if IV is random)

(They are not CCA secure).

Def: An encryption scheme is CCA-secure if an "efficient" (prob. poly time) adversary can win in the following game w.p. $\approx \frac{1}{2}$ ($\frac{1}{2}$ + negl)

Let Enc_K denote the encryption alg w. key K

Let Dec_K " " decryption " " " "

[Note: Enc_K is the alg of the stream cipher, not the block cipher]

<u>Game</u>

Phase I ("Find")

- Adv is given black-box access to Enc_k, Dec_k
- Adv outputs two msgs M_0, M_1 of same length (and state information s).

Phase II ("Guess")

- Adv is given $C \leftarrow Enc_k(M_b)$ for randomly chosen $b \leftarrow \{0,1\}$, and is given black-box access to Enc_k & Dec_k (except on C), and is given state S.

- Adv outputs bit $\hat{b}$, and wins iff $\hat{b} = b$.

<u>CPA - Game</u>: Same except adv is never given oracle to Dec_k (only to Enc_k).

$|\hat{b} - b|$ is called the <u>advantage</u> of the adv.

The encryption scheme is CCA (or CPA) secure if $\forall$ efficient adv, its advantage is negligible.

"pf" that CTR is <u>CPA-secure</u> if E_k is $\underbrace{\text{ideal cipher}}$ indistinguishable from ideal cipher:

Adv can query Enc_k w. many msgs and will learn

$E_k(IV^{(i)} + j)$ $\quad i = 1, \dots, q$ (# of queries) $\quad j = 0, 1, \dots, n$ (# of blocks).

As long as the challenge msg M_b is encrypted using fresh $\{IV^* + j\}$ that will never be reused, $x_0, \dots, x_n$ are ind. from random, and hence serve as a "good" one-time pad. ▨

* A CPA-secure encryption must be randomized or stateful.

CBC is CPA secure if IV is chosen randomly

If IV is not random this encryption can be insecure even if the underlying block cipher is secure (ideally)!

Ex: Suppose IV is unique but is used sequentially, starting w. $IV = 1, 2, \dots$

Then choose M_0, M_1 (arbitrary distinct) for challenge ciphertexts (of length $|k|$).

Upon getting (IV, C), $C = E_k(M_b \oplus IV)$

Query Enc w. M' s.t. $M' \oplus (IV+1) = M_0 \oplus IV$, and receive $(IV+1, C')$. If $C' = C$ then guess $\hat{b} = 0$.

Otherwise, guess $\hat{b} = 1$.

Thm CBC & CTR are <u>not</u> CCA secure.

Pf: Adv picks $M_0 = 0^N$ & $M_1 = 1^N$

Given $c \leftarrow Enc_K(M_b)$, let $C' = 1^{st}$ half of the bits of C (w. same IV).

Since $C' \neq C$, adv is allowed to query Dec_K w. C', which gives 1^{st} half bits of M_b, revealing b.

How do we design CCA-secure schemes?

① Construct a scheme that is only CPA secure

(**Recall**: CBC & CTR are CPA secure if underlying block cipher is ind. from ideal cipher)

② Add authentication.

Message Authentication Code (MAC)

Provides integrity (authenticity), not confidentiality.

called "tag of M"

Alice $\xrightarrow{M,\ MAC_K(M)}$ Bob

M, K   K

Bob recomputes $MAC_K(M)$,
and verifies that it agrees w.
what he received. If not reject
the msg.

- Allows Bob to verify that M originated from Alice, and arrived unmodified.
- Alice & Bob need to share a secret key.
- Orthogonal to confidentiality, typically we do both (encrypt & append MAC on the ciphertext for integrity)

Security for MAC:

<u>Goal</u>: Security against adaptive chosen msg attack:
Adv is given pairs $(M_i, MAC_K(M_i))$ to msgs M_i of his choice, and cannot generate any <u>new</u> M^* w. valid $MAC_K(M^*)$.

* similar to signatures, but in the symmetric key setting.

<u>Note</u>: If MAC has t bits, then Adv can guess w.p. 2^{-t}. Therefore t needs to be large enough.

<u>Thm</u>: CPA-secure encryption scheme + secure MAC $\Rightarrow$ CCA-secure encryption scheme

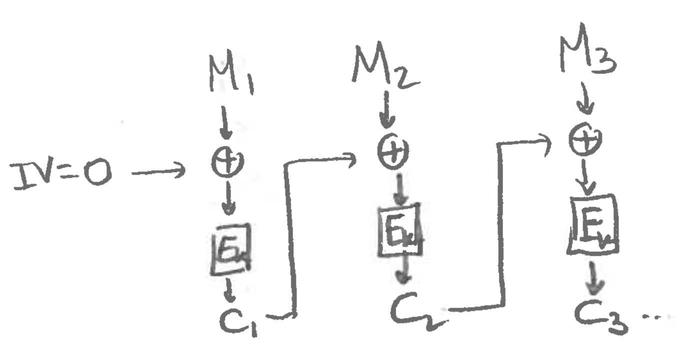
Intuitively, adding a MAC to the ciphertexts makes the decryption oracle useless to the adversary.

How to construct a MAC:

1. From hash functions (HMAC)
2. From block ciphers (CBC-MAC or CMAC)

MAC from block ciphers

<u>1st attempt</u>: $\text{CBC-MAC}_k(M)$: Encrypt M w. CBC mode & $IV = 0$, and output last cipher



Insecure !

Given single block msg M_1 & tag $T_1 = E_k(M_1)$

and single block msg M_2 & tag $T_2 = E_k(M_2)$

T_2 is tag of $M_1 \| M_2 \oplus T_1$

<u>The Fix</u>: Process last block differently:

All blocks use key K_1 and last block uses

key K_2.

$\Bigg\}$ CMAC

<u>Thm</u>: CMAC is a secure MAC, if E_k is an ideal cipher.

* Why does changing the key used in the last block fix security ?

* Why is it important to use <u>fixed</u> IV ?

<u>HW</u>.

Desai [CRYPTO 2000]:

Succinct & efficient CCA secure enc. scheme

(UFE: Unbalanced Feistel Encryption)

$M = (m_1, \ldots, m_n)$ sequence of blocks (length b)

$K = (K_1, K_2, K_3)$ three independent keys for the block cipher.

$Enc_K(M)$:

① Compute $(r, c_1, \ldots, c_n)$ using CTR mode w. secret key K_1:

$r \leftarrow \{0,1\}^b$

$x_i = E_{K_1}(r \oplus i)$ $\quad i \in [n]$

$c_i = m_i \oplus x_i$

② Compute CMAC of $(c_1, \ldots, c_n)$ w.r.t. secret keys K_2, K_3.

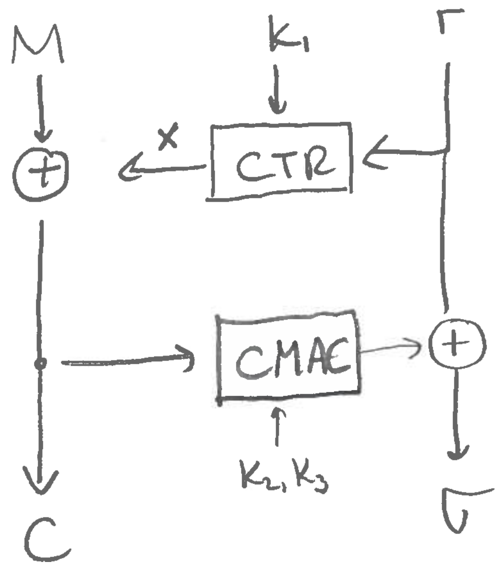
$z_0 = 0^b$

$z_i = E_{K_2}(c_i \oplus z_{i-1})$ $\quad i \in [n-1]$

$z_n = E_{K_3}(c_n \oplus z_{n-1})$ ← last block uses K_3

③ Let $\sigma = r \oplus z_n$

output $(c_1, \ldots, c_n, \sigma)$.



← Unbalanced Feistel structure, thus called Unbalanced Feistel Enc (UFE).

- Encryption can be done in a single pass over the data ("online" property).

  Decryption requires two passes
  - First to compute z_n (CMAC of $C = (c_1, \ldots, c_n)$).
  - Compute $r = \sigma \oplus z_n$
  - Decrypt $(r, c_1 \ldots c_n)$ to get M.

- Provides CCA security

  Does not provide authenticity.

- Length of ciphertext $|C, \sigma| = |M| + b$

  single block