Today:

Continue: symmetric encryption & authentication

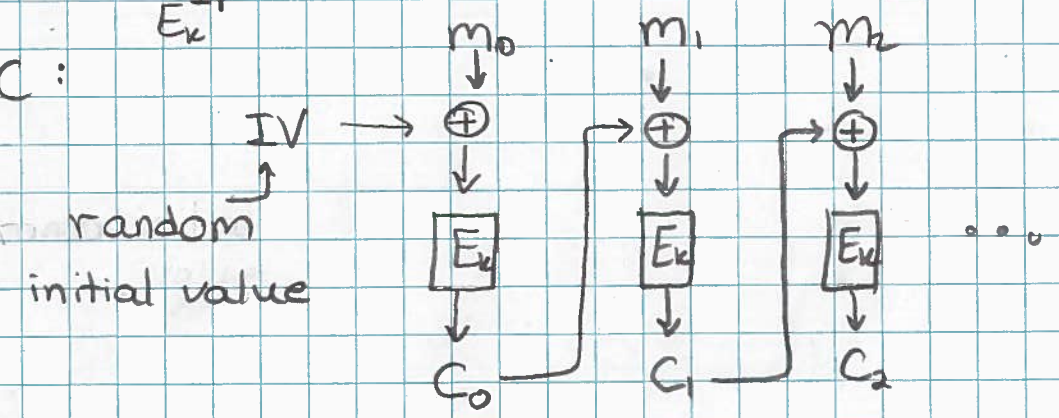
- Cipher Block Chaining (CBC) mode
- CCA security
- Message Authentication Codes (MACs)

Begin - Finite fields
- Shamir Secret Sharing

## Cipher Block Chaining (CBC) Mode

Let $(E_k, D_k)$ be a block cipher ($D_k = E_k^{-1}$)

CBC:




Output IV, $(C_0, C_1, C_2, \ldots)$

* If msg is not of length which is a multiple of

block length then pad (eg., add 10...0 to each msg).

Decrypt: Using $D_k = E_k^{-1}$ in the obvious way.

Claim: If $(E_k, D_k)$ is an ideal block cipher (i.e., random permutation), then CBC mode is a CPA secure encryption scheme (assuming IV is random).

Def: An encryption scheme $(Gen, Enc, Dec)$ (Gen: key generation alg) is CPA secure if $\forall m_0, m_1$ s.t. $|m_0| = |m_1|$ $\forall$ "eff." (poly time) $A$

$$A^{Enc_k}(Enc_k(m_0)) \approx A^{Enc_k}(Enc_k(m_1))$$

$A$ is given black-box access to $Enc_k$.

Actually, $A$ can choose $m_0, m_1$ after querying $Enc_k$

Intuitively: CBC enc. of any msg $(m_0, m_1, \ldots)$ is a random CT $(c_0, c_1, \ldots)$ ind. of $(m_0, m_1 \ldots)$ (if $(E_k, D_k)$ is an ideal cipher).

Randomness of IV is needed to argue that it remains random even given oracle access to $Enc_k$

A stronger notion of security: CCA security

Chosen Ciphertext Attack

**Def:** An encryption scheme (Gen, Enc, Dec) is CCA secure if $\forall m_0, m_1$ s.t. $|m_0| = |m_1|$

$\forall$ efficient $\mathcal{A}$

$$\mathcal{A}^{Enc_k, Dec_k}(Enc_k(m_0)) \approx \mathcal{A}^{Enc_k, Dec_k}(Enc_k(m_1))$$

$\mathcal{A}$ is given black-box access to both $Enc_k$ & $Dec_k$ for $k \leftarrow Gen$.

Moreover $\mathcal{A}$ can choose $m_0$ & $m_1$ after querying $Enc_k$ & $Dec_k$ but cannot send its exact input $Enc_k(m_b)$ as oracle query to $Dec_k$

**Claim:** CBC is not CCA secure.

(and neither are ECB or CTR)

**Pf:** $\mathcal{A}$ picks $m_0 = 0^n$ & $m_1 = 1^n$

Given $c \leftarrow Enc_k(m_b)$ let $c'$ = 1st half of the bits of $c$ (w. same IV).

A queries $Dec_k$ with $c'$ (this is allowed since $c' \neq c$)

which gives 1st half of the bits of $m_b$, revealing $b$.

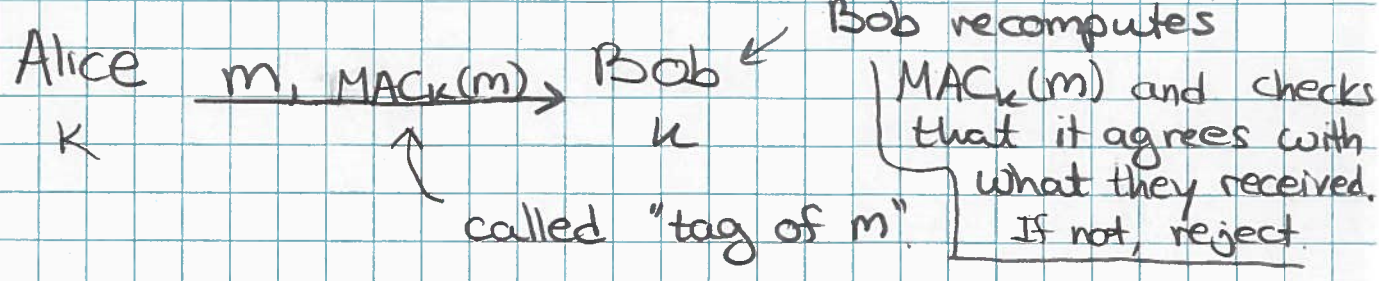
## How do we design CCA secure schemes?

① Construct a CPA secure scheme (eg. CBC).

② Add authentication. (so that $Dec_k$ will only decrypt msgs that are "authenticated")

## Message Authentication Code (MAC)

Provides integrity (authenticity), not confidetiality.




- 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 of MAC

**Def**: A MAC is secure against adaptive chosen msg attacks if $\forall$ eff $A$ given pairs $(m_i, MAC_k(m_i))$ for any msgs $m_i$ of their choice, cannot generate any new $m^*$ with valid $MAC_k(m^*)$

(Jumping ahead: MACs are like digital signatures but in the symmetric key setting)

**Note**: If MAC generates tags of length $t$, then Adv can guess w.p. $2^{-t}$. Therefore $t$ needs to be sufficiently large.

**Thm**: CPA secure encryption scheme + secure MAC $\Rightarrow$ CCA secure encryption scheme

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

## How to construct a MAC

① From hash functions (HMAC)

② From block ciphers (CBC-MAC or CMAC).

## CBC-MAC

$CBC\text{-}MAC_K(m)$ : Encrypt m w. CBC mode with IV = 0 & output only last cipher but the key $K_2$ used for the last block is different from the key $K_1$ used for all other blocks !

(Both $K_1$ & $K_2$ are random & ind.)

HW
- Why does $K_2$ need to be different than $K_1$ ?
- Why isn't IV random ?

# Finite Fields & Shamir Secret Sharing

**Def:** A field is defined by a tuple $(S, +, \cdot)$ s.t.

* $S$ is a set containing "0" & "1".

* $(S, +)$ is an abelian (commutative) group with identity $0$:

group laws:
$$\begin{cases} (a+b)+c = a+(b+c) & \forall a,b,c \in S \quad \text{(associative)} \\ a+0 = 0+a = a & \forall a \in S \quad \text{(identity 0)} \\ \forall a \in S \ \exists b \in S \text{ st. } a+b = 0 & \text{(inverse)} \end{cases}$$
$$a+b = b+a \quad \forall a,b \in S \quad \text{(commutative)}$$

* $(S^*, \cdot)$ is an abelian (commutative) group with identity $1$:

$S^* = S \setminus \{0\}$

group laws:
$$\begin{cases} (a \cdot b) \cdot c = a \cdot (b \cdot c) & \forall a,b,c \in S \quad \text{(associative)} \\ a \cdot 1 = 1 \cdot a = 1 & \forall a \in S \quad \text{(identity 1)} \\ \forall a \in S^* \ \exists b \in S^* \text{ st. } a \cdot b = 1 & \text{(inverse)} \end{cases}$$
$$a \cdot b = b \cdot a \quad \text{(commutative)}$$

Examples $\mathbb{R}$ (reals), $\mathbb{C}$ (complex) } familiar fields.

These are finite fields (i.e., fields w. infinitely many elements).

In crypto, we usually work w. finite fields, where $|S|$ is finite.

Example $(\mathbb{Z}_p, +, \cdot)$ where $+, \cdot$ are mod $p$.
$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$

Thm: $\exists$ finite field w. $q$ elements if and only if $q = p^k$ for some prime $p$ and integer $k \geq 1$.

Moreover, for every such $q$ there is a unique field consisting of $q$ elements, denoted by $GF(q)$
Galois Field

$GF(p)$ for prime $p$ is $(\mathbb{Z}_p, +, \cdot)$, where $+$ & $\cdot$ are mod $p$.