Lecture 3. Symmetric encryption

Passive adversaries, small shared secret

Bruno Grenet

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

Introduction to cryptology
Université Grenoble Alpes – IM²AG
M1 INFO, MOSIG & AM

Block ciphers are not enough

Block ciphers offer

- One-to-one (deterministic) encryption
- Fixed-size messages

We need

- One-to-many (non-deterministic) encryption
- Variable-size messages

Block ciphers are not enough

Block ciphers offer

- One-to-one (deterministic) encryption
- Fixed-size messages

We need

- One-to-many (non-deterministic) encryption
- Variable-size messages

Symmetric encryption scheme

$$\begin{cases} \mathsf{Enc} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^* \\ \mathsf{Dec} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^* \end{cases}$$

- Enc is a *randomized* encryption algorithm
- Dec is a (deterministic) decryption algorithm

Correctness: for all $k \in \{0,1\}^\kappa$, $m \in \{0,1\}^*$ and $c \leftarrow \mathsf{Enc}_k(m)$, $\mathsf{Dec}_k(c) = m$

Efficiency: for all $k \in \{0,1\}^\kappa$, $m \in \{0,1\}^*$ and $c \leftarrow \mathsf{Enc}_k(m)$, $|c| \simeq |m|$

Block ciphers are not enough

Block ciphers offer

- One-to-one (deterministic) encryption
- Fixed-size messages

We need

- One-to-many (non-deterministic) encryption
- Variable-size messages

Symmetric encryption scheme

$$\begin{cases} \mathsf{Enc} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^* \\ \mathsf{Dec} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^* \end{cases}$$

- Enc is a *randomized* encryption algorithm
- Dec is a (deterministic) decryption algorithm

Correctness: for all $k \in \{0,1\}^\kappa$, $m \in \{0,1\}^*$ and $c \leftarrow \mathsf{Enc}_k(m)$, $\mathsf{Dec}_k(c) = m$

Efficiency: for all $k \in \{0,1\}^\kappa$, $m \in \{0,1\}^*$ and $c \leftarrow \mathsf{Enc}_k(m)$, $|c| \simeq |m|$

- How to build symmetric encryption schemes?
- What are *good* encryption schemes?

From block ciphers to symmetric encryption schemes

The tool: modes of operations

- Transforms a block cipher into a *symmetric encryption scheme*

$$E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n \rightsquigarrow \begin{cases} \text{Enc} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^* \\ \text{Dec} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^* \end{cases}$$

- A mode is *good* if it turns *good BCs* into *good encryption schemes*

Another approach: from stream ciphers

- Basic (incomplete) idea:
  - Use one-time pad with *pseudo-random* bits
  - Produce the pseudo-random bits on the fly
- In terms of security:
  - block cipher $\leftrightsquigarrow$ pseudo-random permutation
  - stream cipher $\leftrightsquigarrow$ pseudo-random generator

Contents

Reminder: IND-CPA game

IND-CPA game for Enc : $\mathcal{K} \times \mathcal{M} \to \mathcal{M}$

Challenger draws $k \twoheadleftarrow \mathcal{K}$

Adversary has *oracle* access to $\mathrm{Enc}_k(\cdot)$: on query x_i, gets $c_i \leftarrow \mathrm{Enc}_k(x_i)$

Adversary creates two equal-length messages m_0 and m_1

Challenger draws $b \twoheadleftarrow \{0,1\}$ and computes $c \leftarrow \mathrm{Enc}_k(m_b)$

Adversary returns $\hat{b}$ (*tries to guess* b)

Remarks

- Oracle access during the whole experiment
- Equal-length messages $\rightsquigarrow$ message length not hidden!
  - Impossible to hide if messages of any length
  - Use padding beforehand if message length is sensitive

Reminder: IND-CPA advantage

IND-CPA advantage of an adversary A

$$\mathrm{Adv}^{\mathrm{IND-CPA}}_{\mathrm{Enc}}(\mathcal{A}) = \left|\Pr\left[\mathcal{A}^{\mathrm{Enc}_k} \to 1 \middle| b = 1\right] - \Pr\left[\mathcal{A}^{\mathrm{Enc}_k} \to 1 \middle| b = 0\right]\right|$$

- Equal to $|\Pr[\hat{b} = 1 | b = 1] - \Pr[\hat{b} = 1 | b = 0]|$ and to $|2\Pr[\hat{b} = b] - 1|$
- Extremal cases:
  - Guessing $\hat{b}$ at random $\rightsquigarrow$ advantage 0
  - Resource-unbounded $\mathcal{A} \rightsquigarrow$ advantage 1

$q = 0, t = 1 \Rightarrow \mathrm{Adv}^{\mathrm{IND-CPA}}_{\mathrm{Enc}}(0,1) = 0$

$\mathrm{Adv}^{\mathrm{IND-CPA}}_{\mathrm{Enc}}(\text{"}+\infty\text{"}, \text{"}+\infty\text{"}) = 1$

IND-CPA advantage function

$$\mathrm{Adv}^{\mathrm{IND-CPA}}_{\mathrm{Enc}}(q, t) = \max_{\mathcal{A}_{q,t}} \mathrm{Adv}^{\mathrm{IND-CPA}}_{\mathrm{Enc}}(\mathcal{A}_{q,t})$$

where $\mathcal{A}_{q,t}$ is an alg. that runs in time $\leq t$ and makes $\leq q$ queries to the challenger

Comments on IND-CPA security

- No formal definition of IND-CPA secure, only a measure *(but in asymptotic security)*
- IND-CPA $\Rightarrow$ non-determinism (A can query $\mathrm{Enc}_k(m_0)$ and $\mathrm{Enc}_k(m_1)$)
- IND-CPA $\Rightarrow$ the adversary cannot compute any single bit of the message
- IND-CPA $\Rightarrow$ the adversary can compute *very few* information on the message

Stronger security notions

- Indistinguishability under chosen ciphertext attack
  - Access to both an encryption oracle and a decryption oracle
  - 2 variants: non-adaptative (IND-CCA) or adaptative (IND-CCA2)
- Indistinguishability for multiple encryptions either CPA or CCA
  - Challenger draws $b \twoheadleftarrow \{0,1\}$
  - Adversary submits *pairs* of challenges (m_i^0, m_i^1) and gets $c_i \leftarrow \mathrm{Enc}_k(m_i^b)$
  - Adversary must find b

Contents

Goal

$$E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n \rightsquigarrow \begin{cases} \text{Enc} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^* \\ \text{Dec} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^* \end{cases}$$

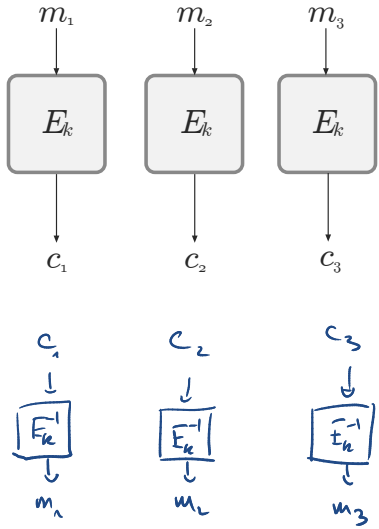
- E is made to encrypt one block of data
- Enc should encrypt any number of blocks

$\to$ Use E several times to encrypt a message $m \in \{0,1\}^*$

Desired properties

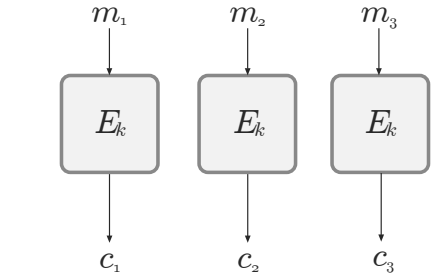
- Security:
  - E *good* $\implies$ Enc *good*
  - Low (S)PRP advantage $\implies$ low IND-CPA advantage
- Efficiency:
  - Efficient encryption and decryption — if E is efficient
  - Ciphertext not too large compared to message

Obvious (bad) idea: Electronic Code Book (ECB)



Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

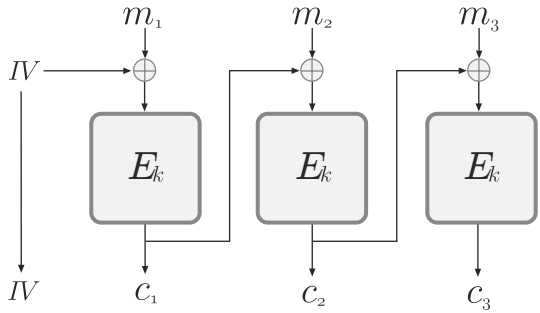
Obvious (bad) idea: Electronic Code Book (ECB)

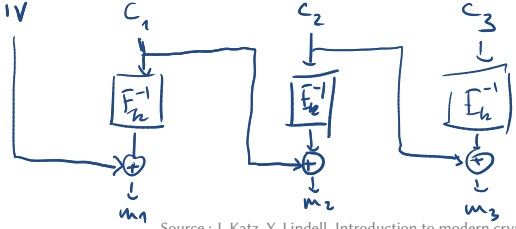


Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

Source : Wikipédia (modif.)

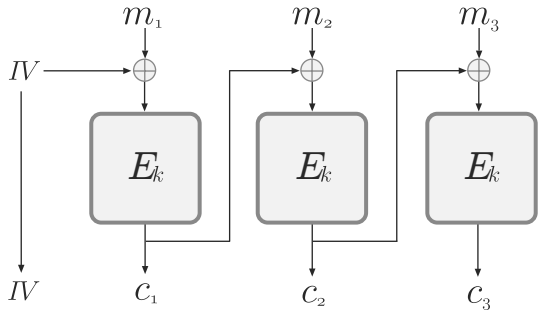
First (real) example of mode of operation: Cipher Block Chaining (CBC)





Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

First (real) example of mode of operation: Cipher Block Chaining (CBC)

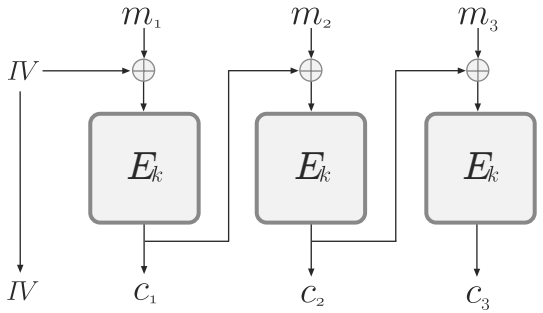


- IV: *random* initialization vector in $\{0,1\}^n$
- Input: $m = m_1 \| \cdots \| m_\ell$ — padding if needed
- Output: $c = IV \| c_1 \| \cdots \| c_\ell$ — size $n(\ell + 1)$

- IND-CPA security if E is a good PRP and IV truly random

Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

First (real) example of mode of operation: Cipher Block Chaining (CBC)



Adversary when IV is not uniform

1. One-block query $m \to r \| c$ where $c = E_k(m \oplus r)$ *r is IV*
2. *Guess* the next IV: r'
3. Challenges $m_0 = m \oplus r \oplus r'$ and m_1 uniform $\to r'' \| c_b$ where $c_b = E_k(m_b \oplus r'')$
4. If the guess is correct ($r' = r''$), return $\begin{cases} b = 0 & \text{if } c = c_b \\ b = 1 & \text{otherwise} \end{cases}$ (if $r' \neq r''$, *failure*)

↳ $c_b = E_k(m_b \oplus r') = \begin{cases} E_k(m \oplus r) = c & \text{if } b = 0 \\ \text{random value} & \text{if } b = 1 \end{cases}$

Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

Generic CBC collision attack

Observation

- For fixed k, E_k is a permutation $\rightarrow E_k(x) = E_k(y) \iff x = y$
- In CBC, inputs to E_k are of the form $m_i \oplus c_{i-1}$ $\qquad c_0 = IV$

$$\underbrace{E_k(m_i \oplus c_{i-1})}_{c_i} = \underbrace{E_k(m'_j \oplus c'_{j-1})}_{c'_j} \iff m_i \oplus c_{i-1} = m'_j \oplus c'_{j-1}$$

Consequence

- Assume we get two identical ciphertext blocks:

$$\begin{aligned} c_i = c'_j &\iff E_k(m_i \oplus c_{i-1}) = E_k(m'_j \oplus c'_{j-1}) \\ &\iff m_i \oplus c_{i-1} = m'_j \oplus c'_{j-1} \\ &\iff c_{i-1} \oplus c'_{j-1} = m_i \oplus m'_j \end{aligned}$$

- $c_{i-1} \oplus c'_{j-1}$ reveals information about m_i and m'_j
  $\Rightarrow$ breaks IND-CPA security *no matter how good E!*

Probability to get collisions?

Assumption

The distribution of the $(m_i \oplus c_{i-1})$ is approx. uniform

- If c_0 is the IV, it has to be approx. uniform
- If c_{i-1} is a ciphertext, non (approx.) uniformity would imply an attack

Birthday bound

Draw $y_1, \ldots, y_q$ uniformly from a size-N set, with $q \leq \sqrt{2N}$. Then

$$\frac{q(q-1)}{4N} \leq 1 - e^{-q(q-1)/2N} \leq \Pr\left[\exists i \neq j, y_i = y_j\right] \leq \frac{q(q-1)}{2N}$$

Consequence

- Collision found w.h.p. if $q \simeq \sqrt{N}$
- For CBC: Collision w.h.p. after observing $\simeq 2^{n/2}$ ciphertext blocks
- Note: does not depend on key size κ

Proof of the birthday upper bound

If $y_1, \ldots, y_q \leftarrow S$ with $|S| = N$, then $\Pr[\exists i \neq j, y_i = y_j] \leq \frac{q(q-1)}{2N} = \frac{\binom{q}{2}}{N}$

- $\Pr[\exists i \neq j, y_i = y_j] = \Pr\left[\bigvee_{i \neq j} y_i = y_j\right] \underset{\text{union bound}}{\leq} \sum_{i \neq j} \Pr[y_i = y_j]$
- $\Pr[y_i = y_j] = 1/N$
- $\Pr[\exists i \neq j, y_i = y_j] \leq \sum_{i \neq j} \frac{1}{N} = \binom{q}{2}/N$.

Proof of the birthday lower bound

If $y_1, \ldots, y_q \twoheadleftarrow S$ with $|S| = N$, then $\Pr[\exists i \neq j, y_i = y_j] \geq 1 - e^{-\frac{q(q-1)}{2N}}$

$(\geq \frac{q(q-1)}{4N}$ if $q \leq \sqrt{2N})$ admitted

- $p = \Pr[\forall i \neq j,\ y_i \neq y_j] = \Pr[y_2 \neq y_1 \wedge y_3 \notin \{y_1, y_2\} \wedge \cdots \wedge y_q \notin \{y_1, \ldots, y_{q-1}\}]$ ($y_2 \notin \{y_1\}$)
- E_i : $y_i \notin \{y_1, \ldots, y_{i-1}\}$ and $\forall j, k < i \quad y_j \neq y_k$
- $p = \Pr[\overline{E}_2 \wedge \overline{E}_3 \wedge \cdots \wedge \overline{E}_q] = \prod_{i=2}^{q} \Pr[\overline{E}_i]$ by independence.
- $\Pr[\overline{E}_i] = \frac{N-i+1}{N} = 1 - \frac{i-1}{N}$
- $p = \prod_{i=2}^{q} 1 - \frac{i-1}{N} = \prod_{i=1}^{q-1} (1 - i/N) \leq \prod_{i=1}^{q-1} e^{-i/N} = e^{-\frac{1}{N}\sum_{i=1}^{q-1} i} = e^{-\frac{q(q-1)}{2N}}$ ($1+x \leq e^x$)

The birthday attack against CBC

Adversary $\mathcal{A}_{\text{BIRTHDAY}}$

- Sends two messages with $\simeq 2^{n/2}$ blocks each
  - m_0 with only zeroes
  - m_1 with pairwise distinct blocks
- Gets back $c = \text{Enc}_k(m_b)$
  - If there are two blocks $c_i = c_j$, return 0 if $c_{i-1} \oplus c_{j-1} = 0 \cdots 0$, 1 otherwise
  - If not, return 0 or 1 at random

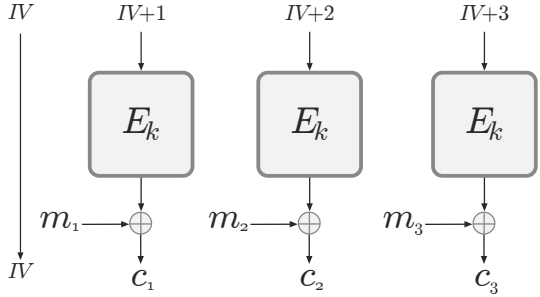
Analysis

- Correct answer if there exists $i \neq j$ s.t. $c_i = c_j$, since $c_{i-1} \oplus c_{j-1} = m_i \oplus m_j$ ✓ $m = m_b$
- $\Pr[\exists i \neq j, c_i = c_j] \gtrsim \frac{1}{4} \rightarrow \text{advantage} \gtrsim \frac{1}{4}$
- Time to find collisions: $O(2^{n/2})$

Conclusion

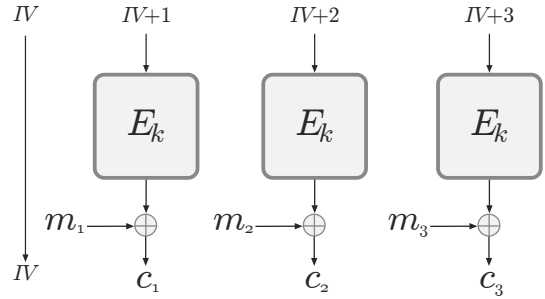
- $\text{Adv}^{\text{IND-CPA}}_{\text{Enc}-CBC}(2^{n/2}, 2^{n/2}) \geq \text{Adv}^{\text{IND-CPA}}_{\text{Enc}-CBC}(\mathcal{A}_{\text{BIRTHDAY}}) \gtrsim \frac{1}{4}$
- CBC mode should not be used for too long with the same key!

Second example of mode of operation: Counter (CTR)



Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

Second example of mode of operation: Counter (CTR)



- IV: *random* initialization vector in $\{0,1\}^n$
- Input: $m = m_1 \| \cdots \| m_\ell$
- Output: $c = IV \| c_1 \| \cdots \| c_\ell$ — size $n(\ell+1)$
- Parallel encryption (fast!) — similar to a *stream cipher*
- Also sensitive to birthday bound
- IND-CPA security from PRF security — variant of PRP security

Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

IND-CPA security for CTR: sketch of the proof

- PRF security: similar to PRP but with random function rather than permutation

  E_k is PRF-secure: for any alg $A_{q,t}$, $\left|\Pr\left[A_{q,t}^{E_k} \to 1\right] - \Pr\left[A_{q,t}^{f} \to 1\right]\right| \leq Adv^{PRF}_{E_k}(q,t)$

  (f: random function)

- Let A be an adv. for $CTR[E_k]$ in the IND-CPA game, that makes q queries

  $$\left|\Pr\left[A^{CTR[E_k]} \to b\right] - \Pr\left[A^{CTR[f]} \to b\right]\right| \leq Adv^{PRF}_{E_k}(q',\epsilon)$$

- Claim $\Pr\left[A^{CTR[f]} \to b\right] = 1/2 + \frac{q'\ell}{2^n}$ when q' is the total length of the q queries, ℓ is the length of m_0, m_1

  - Queries $x_i = x_i^1 \| \cdots \| x_i^{\ell_i} \rightsquigarrow y_i = IV_i \| y_i^1 \| \cdots \| y_i^{\ell_i}$
  - $m_0 = m_0^1 \| \cdots \| m_0^\ell$, $m_1 = m_1^1 \| \cdots \| m_1^\ell$, $c = IV \| c^1 \| \cdots \| c^\ell$
  - If there is no collision $IV + k = IV_i + j$, $\Pr\left[A^{CTR[f]} \to b\right] = 1/2$
  - $\Pr\left[\exists i,j,k,\ IV + k = IV_i + j\right] = \Pr\left[\exists i,j,k,\ IV = IV_i + j - k\right] = \frac{\sum \ell_i \cdot \ell}{2^n} = \frac{q'\ell}{2^n}$

  $\Pr\left[A^{CTR[f]} \to b\right] \leq 1/2 + \frac{q'\ell}{2^n}$

Finally

Modes of operations

- A *good* mode of operation turns a *good* block cipher into a *good* symmetric encryption scheme
- Different mode of operations require different quality for the block cipher
  - *Good* PRP
  - *Good* PRF
  - Ideal Block Cipher
- Proofs of security $\rightarrow$ reductions between problems
- Usually: need more $\rightarrow$ *ad hoc* analysis of the resulting system

Other symmetric encryption schemes

- Other modes of operations — OFB, CFB
- Stream ciphers — *Wifi, 5G, …*

Conclusion

Symmetric encryption, as we saw it

- Two ingredients:
  - a block cipher — fixed-size, deterministic
  - a mode of operation — variable-size, non-deterministic
- Security notions:
  - PRP advantage — block cipher
  - IND-CPA advantage — symmetric encryption
- More advanced security definitions:
  - strong PRP adv., (strong) PRF adv., ideal block cipher
  - IND-CCA, IND-CCA2, multiple encryptions

In practice

- Block cipher: mainly AES, with key size 128 bits
- Modes of operations: *e.g.* extension of CTR in TLS

Final words: **Definitions and proofs are important!**