Modes of Operations.

Elena Kirshanova

Course “Information and Network Security”
Lecture 4
24 марта 2020 г.

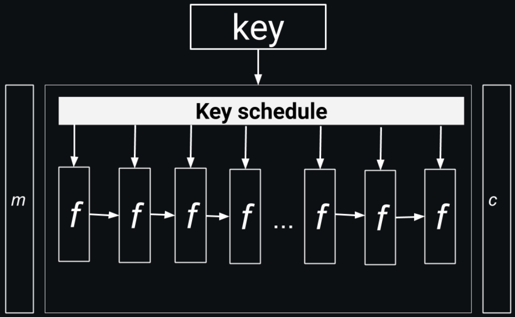
Recap: Block ciphers

- Most popular primitive for symmetric encryption
- Core element: a public function f

$$f(x,k) \quad x \in \mathcal{M},\ k \in \mathcal{K} \text{ such that}$$

f is efficient and secure⋆

- we iterate f over several rounds

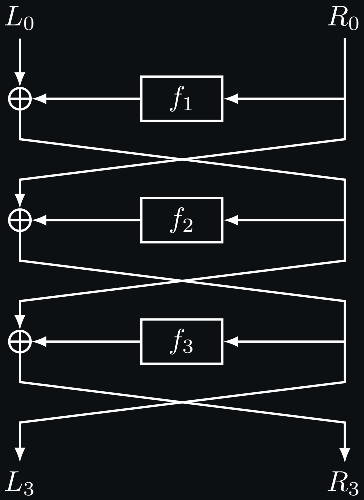


⋆ a secure block cipher is non-trivial to define

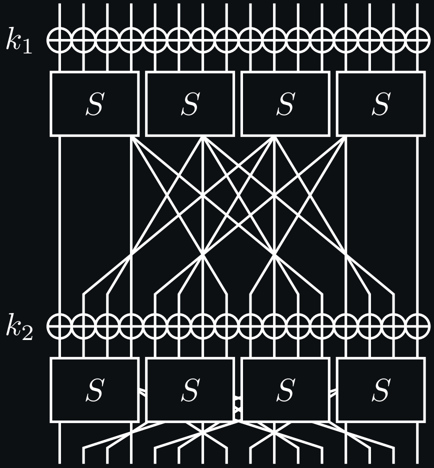
Recap: Block ciphers

There are two main design principals of rounds

Feistel cipher



Substitution Permutation Network



Recap: Block ciphers

- Feistel cipher
  - Usually requires more rounds to achieve ‘good mixing’
  - Easy to invert: iterate in reverse

  Examples: DES, ГОСТ 28147-89

- Substitution-Permutation Network (SPN).
  Подстановочно-перестановочная сеть
  - Used in modern protocols
  - Inversion is non-trivial

  Examples: AES, ГОСТ 34.12-2018

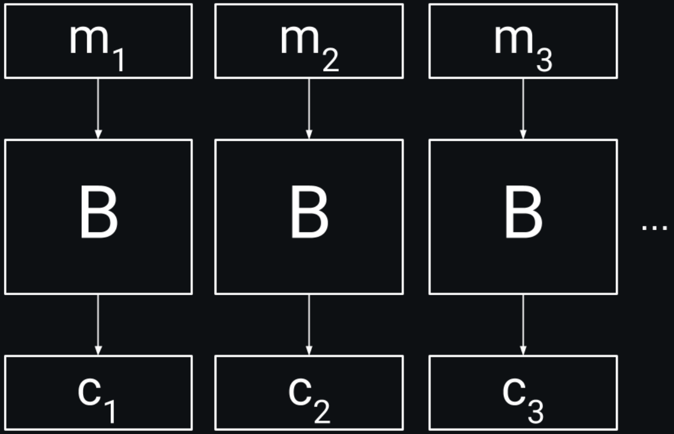
How to use a block cipher correctly?

Modes of operation.

Electronic Block Code (EBC)

Let $m = (m_1, m_2, m_3, ...)$

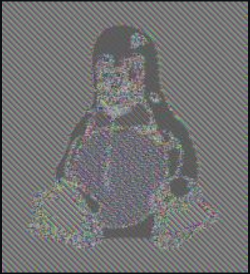
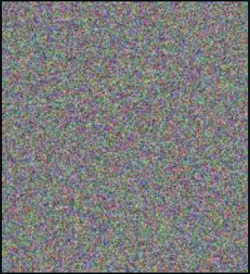
A naive way to use a block cipher B



This is INSECURE! If $m_1 = m_2$ then $c_1 = c_2$

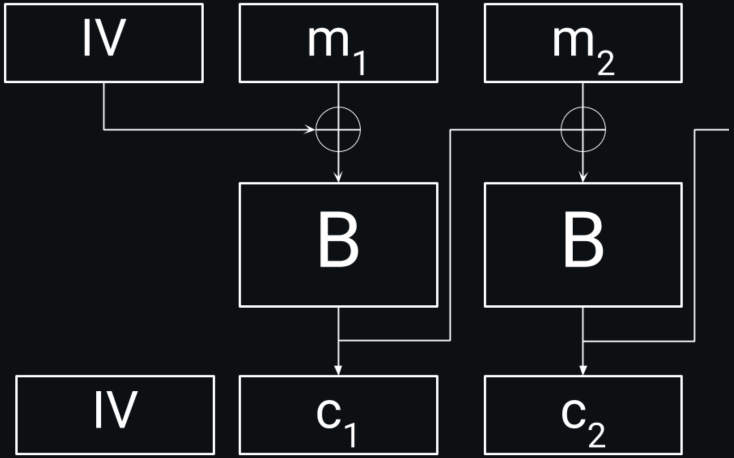
Insecurity of EBC

If $m_1 = m_2$ then $c_1 = c_2$

Cipher Block Chain (CBC)

IV – Initial Vector – a random bit string



IV is a part of a ciphertext, i.e., publicly known

Security of Cipher Block Chain (CBC)

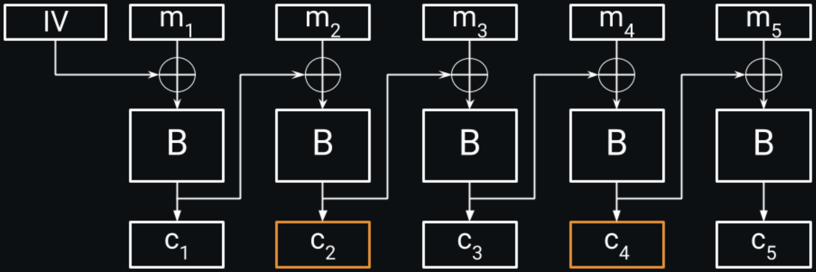
- The IV must be unpredictable (if an attacker predicts IV, encryption with CBC is not secure).
  Known vulnerability in TLS 1.1 (ciphertext of a message was used as IV for the next message).

Security of Cipher Block Chain (CBC)

- The IV must be unpredictable (if an attacker predicts IV, encryption with CBC is not secure).
  Known vulnerability in TLS 1.1 (ciphertext of a message was used as IV for the next message).
- IV must be updated

Security of Cipher Block Chain (CBC)

Assume we encrypt under the same IV a very long message $m = (m_1, \ldots, m_t)$ for $t > 2^{n/2}$ where n is the block length ($n = 128$ for AES, GOST'15)



Birthday paradox: after seeing $2^{n/2}$ cipher-text blocks c_i's, with high probability two of them will be equal, e.g., $c_2 == c_4$ Therefore,

$$c_1 \oplus m_2 == c_3 \oplus m_4$$

Statistical attacks can be applied.

Birthday Paradox

Q: Is it more likely that some two people in the room of 30 people share the same birthday or that no two people in the room share the same birthday?

Birthday Paradox

Q: Is it more likely that some two people in the room of 30 people share the same birthday or that no two people in the room share the same birthday?
Simple calculations* reveal that the 2nd event happens with probability

$$\left(1-\frac{1}{365}\right)\left(1-\frac{2}{365}\right)\left(1-\frac{3}{365}\right)\cdot\ldots\cdot\left(1-\frac{29}{365}\right)\approx 0.294$$

Hence, with probability $> 70\%$ there are two people sharing the same birth date.

$\star$ see any introductory textbook on probability theory

Birthday Paradox

In general, if there are m people and N possible birthdays, the probability that all m have different birthdays is

$$\prod_{i=1}^{m-1} \left(1 - \frac{i}{N}\right) \approx e^{-m^2/2N}$$

Hence, for $m = \sqrt{2N \ln 2}$, the probability that all m people have different birthdays is $1/2$. This probability decreases rapidly when m grows.

Birthday Paradox

In general, if there are m people and N possible birthdays, the probability that all m have different birthdays is

$$\prod_{i=1}^{m-1}\left(1-\frac{i}{N}\right)\approx e^{-m^2/2N}$$

Hence, for $m=\sqrt{2N\ln 2}$, the probability that all m people have different birthdays is $1/2$. This probability decreases rapidly when m grows.

In block ciphers on block length n, we have 2^n possible ciphers. After $m=\mathcal{O}(2^{n/2})$ different cipher blocks c_i's, two of them are equal with constant probability.

Birthday Paradox

In general, if there are m people and N possible birthdays, the probability that all m have different birthdays is

$$\prod_{i=1}^{m-1} \left(1 - \frac{i}{N}\right) \approx e^{-m^2/2N}$$

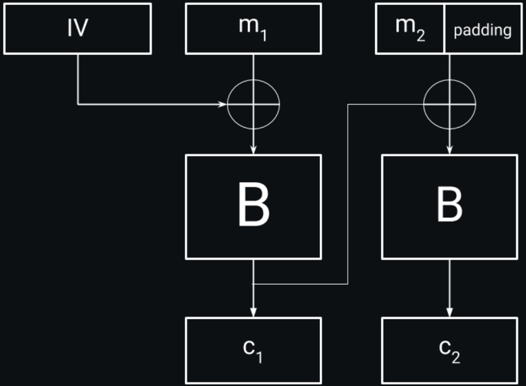
Hence, for $m = \sqrt{2N \ln 2}$, the probability that all m people have different birthdays is $1/2$. This probability decreases rapidly when m grows.

In block ciphers on block length n, we have 2^n possible ciphers. After $m = \mathcal{O}(2^{n/2})$ different cipher blocks c_i's, two of them are equal with constant probability.
For CBC mode: $c_i == c_j$ for $m = (m_1, \ldots, m_t)$, $t \approx 2^{n/2}$:

$$c_{i-1} \oplus m_i == c_{j-1} \oplus m_j$$

Padding for CBC

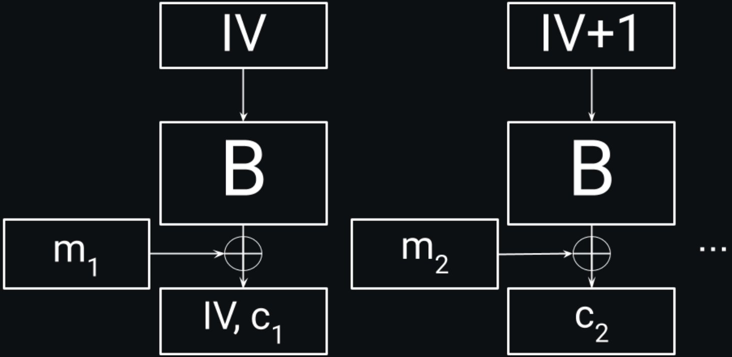
The CBC mode requires padding



Usually n-byte padding is consists of n copies of n: i.e., 5 bytes padding is $5|5|5|5|5$. If m is less than the block-length, we add a dummy block.

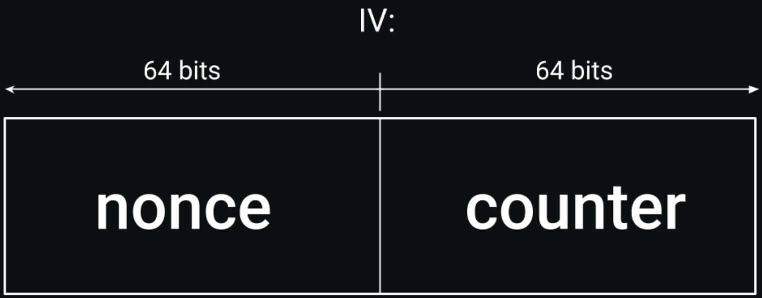
Counter Mode (CTR)

Modern way to use block ciphers
Now IV - initial value of a counter: it is incremented for each new message block. Only the initial value of IV is transmitted.



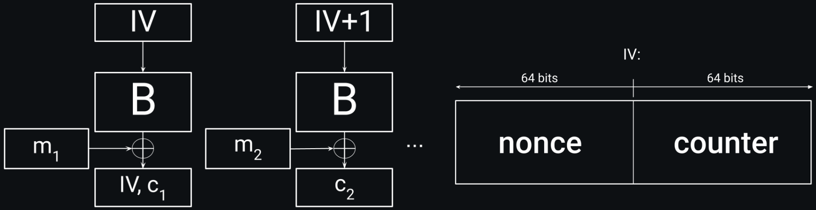
This is a way to turn a block cipher into a stream cipher

Example of a Shape of IV



- Nonce should be unpredictable (a 64-bit output of a PRG) and should never repeat for the same key k
- Counter increments for every message block
- Do to need to transmit the counter in protocols that guarantee in-order delivery (e.g., https)
- Can use one nonce for at most 2^{64} message blocks, i.e., refresh the nonce after 2^{64} encryptions

Counter Mode (CTR)



- Nonce is known to both encryptor and decryptor
- Advantage: Simple decryption routine
- Advantage: Can be parallelized (unlike CBC)
- Advantage: No need to use padding

Take-away

1. DO NOT use the EBC mode

2. The CBC mode, used in old TLS, is inferior to the CTR mode

3. Use the CTR mode in your constructions

Programming assignment

Task: encrypt a text file with AES

Details and useful links are in the instructions file

Send your questions and finished assignments to

`elenakirshanova@gmail.com`

Feedback

Please leave your anonymous feedback at

`https://docs.google.com/forms/d/e/1FAIpQLSfVLhzxzbuxhAawoESWaCL50146ktDwVRXMLK5FeXzFTzuGTA/viewform?usp=sf_link`