Introduction to cryptography

Quiz

Gilles Van Assche
Olivier Markowitch

INFO-F-405
Université Libre de Bruxelles
2020-2021

Perfect secrecy

Which assertion is correct?
(Note: unconditional security = perfect secrecy.

- A A cipher is unconditionally secure **implies that** the secret key is at least as long as the plaintext.
- B A cipher is unconditionally secure **as soon as** the secret key is at least as long as the plaintext.
- C A cipher is unconditionally secure **if and only if** the secret key is at least as long as the plaintext.

Perfect secrecy

Which assertion is correct?
(Note: unconditional security = perfect secrecy.

- A A cipher is unconditionally secure **implies that** the secret key is at least as long as the plaintext.
- B A cipher is unconditionally secure **as soon as** the secret key is at least as long as the plaintext.
- C A cipher is unconditionally secure **if and only if** the secret key is at least as long as the plaintext.

The correct answer is **A**. It is easy to build a cipher with a key longer than the plaintext that does not achieve perfect secrecy.

Not-so-one-time pad

What happens if the one-time pad is incorrectly used and that two distinct plaintexts are encrypted with the same key?

A The key is compromised.

B The two plaintexts are revealed.

C The difference between the two plaintexts is revealed.

D The authenticity of the plaintext is compromised.

Not-so-one-time pad

What happens if the one-time pad is incorrectly used and that two distinct plaintexts are encrypted with the same key?

- A The key is compromised.
- B The two plaintexts are revealed.
- C The difference between the two plaintexts is revealed.
- D The authenticity of the plaintext is compromised.

The correct answer is **C**.

Computational security

Assume an adversary performs an exhaustive key search on a huge network of 10^9 computers, each capable of testing 10^9 keys per second. After about how much time will a 128-bit key typically be found?

- A A few seconds.
- B A few days.
- C A few years.
- D A few centuries.
- E A few times the age of the universe.

Computational security

Assume an adversary performs an exhaustive key search on a huge network of 10^9 computers, each capable of testing 10^9 keys per second. After about how much time will a 128-bit key typically be found?

- A A few seconds.
- B A few days.
- C A few years.
- D A few centuries.
- E A few times the age of the universe.

The correct answer is **E**.

Nonce

What does “nonce” stand for?

- A Number used only once
- B Non-committing encryption
- C Network neutrality for confidentiality and encryption

Nonce

What does “nonce” stand for?

- A Number used only once
- B Non-committing encryption
- C Network neutrality for confidentiality and encryption

The correct answer is **A**.

Semantic security / IND-CPA

For a cipher to achieve semantic security (or equivalently, to be IND-CPA secure), which condition is necessary?

- A It must be randomized.
- B It must be randomized (if asymmetric) or it must use a nonce (if symmetric).
- C It must ensure that one cannot recognize whether two identical plaintexts were encrypted with the same key.

Semantic security / IND-CPA

For a cipher to achieve semantic security (or equivalently, to be IND-CPA secure), which condition is necessary?

- A It must be randomized.
- B It must be randomized (if asymmetric) or it must use a nonce (if symmetric).
- C It must ensure that one cannot recognize whether two identical plaintexts were encrypted with the same key.

The correct answer is **C**. Answers A and B are sufficient conditions that ensure the property C.

Primitive

In this course, how is a symmetric crypto *primitive* defined?

A It is an algorithm whose security cannot be proven but must tested with third-party cryptanalysis.

B It is the set of elementary operations that must be performed in an encryption or authentication scheme.

C It is a painter in the Renaissance.

Primitive

In this course, how is a symmetric crypto *primitive* defined?

- A It is an algorithm whose security cannot be proven but must tested with third-party cryptanalysis.
- B It is the set of elementary operations that must be performed in an encryption or authentication scheme.
- C It is a painter in the Renaissance.

The correct answer is **A**.

Mode of operation

What is a mode of operation?

- A The formal security requirements in which an encryption or authentication scheme must operate.
- B An algorithm that implements any type of scheme or another primitive by using a primitive as a black box.

Mode of operation

What is a mode of operation?

- A The formal security requirements in which an encryption or authentication scheme must operate.
- B An algorithm that implements any type of scheme or another primitive by using a primitive as a black box.

The correct answer is **B**.

Salvaging ECB

Assume a user encrypts plaintext using AES-ECB, and the plaintext is highly compressed data. Is this encryption secure in a known plaintext setting?

- A No, it is totally insecure.
- B Yes, it is secure, but up to the birthday bound (2^{64} blocks)
- C Yes, it is secure all the way up to 2^{128} blocks

Salvaging ECB

Assume a user encrypts plaintext using AES-ECB, and the plaintext is highly compressed data. Is this encryption secure in a known plaintext setting?

- A No, it is totally insecure.
- B Yes, it is secure, but up to the birthday bound (2^{64} blocks)
- C Yes, it is secure all the way up to 2^{128} blocks

The correct answer is **B**. ECB will reveal the value of a plaintext block only if the same block occurs. Since the plaintext is highly compressed, they look like random 128-bit values, and information can be revealed only if there is a collision among the plaintext (or ciphertext) blocks.

Rijndael

In Rijndael, if we change one byte in the input block, how many bytes are *guaranteed* to change in the state after 2 rounds?

- A 1
- B 4
- C 8
- D 16

Rijndael

In Rijndael, if we change one byte in the input block, how many bytes are *guaranteed* to change in the state after 2 rounds?

- A 1
- B 4
- C 8
- D 16

The correct answer is **D**.

- After the first MixColumns, 4 bytes in the same column are guaranteed to change.
- ShiftRows will move the 4 changed bytes to different columns.
- The second MixColumns will change 4 bytes in each of the 4 columns.

Sponges

The sponge construction is

A a mode on top of a keystream generator

B a mode on top of a block cipher

C a mode on top of a permutation

D a factory that produces kitchen appliances

Sponges

The sponge construction is

- A a mode on top of a keystream generator
- B a mode on top of a block cipher
- C a mode on top of a permutation
- D a factory that produces kitchen appliances

The correct answer is **C**.

Sponges vs keyed sponges

The difference between a sponge function and a keyed sponge function is:

- A The keyed sponge has one more input, the secret key, that is concatenated to the input string before being absorbed.
- B The keyed sponge allows to alternatively absorb input blocks and request output blocks.

Sponges vs keyed sponges

The difference between a sponge function and a keyed sponge function is:

- A The keyed sponge has one more input, the secret key, that is concatenated to the input string before being absorbed.
- B The keyed sponge allows to alternatively absorb input blocks and request output blocks.

The correct answer is **A**. The keyed sponge construction can be seen as a thin mode layer on top of the plain sponge construction. It is the duplex construction that allows to alternatively absorb input blocks and request output blocks.

Hashing more

SHA-256 is a well-known hash function with 256 bits of output. Let us build the $n = 512$-bit hash function SHA-256+256 this way:

$$\text{SHA-256+256}(x) = \text{SHA-256}(x||0) \;||\; \text{SHA-256}(x||1).$$

What is the collision resistance of SHA-256+256?

- A 64 bits
- B 128 bits
- C 192 bits
- D 256 bits
- E 384 bits
- F 512 bits

Hashing more

SHA-256 is a well-known hash function with 256 bits of output. Let us build the $n = 512$-bit hash function SHA-256+256 this way:

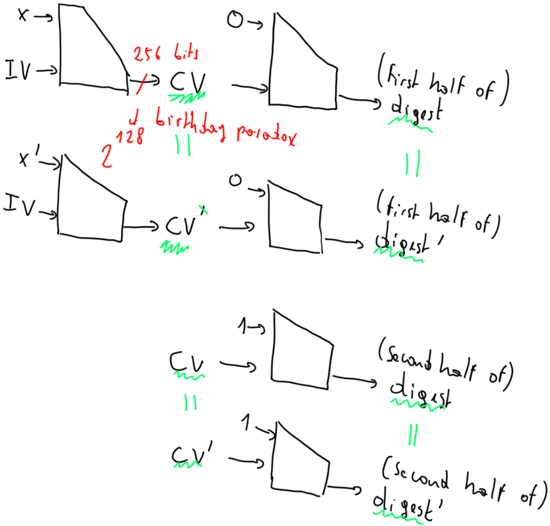
$$\text{SHA-256+256}(x) = \text{SHA-256}(x||0) \; || \; \text{SHA-256}(x||1).$$

What is the collision resistance of SHA-256+256?

- A 64 bits
- B 128 bits
- C 192 bits
- D 256 bits
- E 384 bits
- F 512 bits

The correct answer is **B**. The attacker can find a collision in the chaining value (CV) when processing *x*. The size of the CV is 256 bits, so the collision resistance is 128 bits.

Hashing more



More hashing

SHA-256 is a well-known hash function with 256 bits of output. Let us now build the $n = 512$-bit hash function SHA-256+256 differently:

$$\text{SHA-256+256}(x) = \text{SHA-256}(0||x) \mid\mid \text{SHA-256}(1||x).$$

What is the collision resistance of (this new) SHA-256+256?

- A 64 bits
- B 128 bits
- C 192 bits
- D 256 bits
- E 384 bits
- F 512 bits

More hashing

SHA-256 is a well-known hash function with 256 bits of output. Let us now build the $n = 512$-bit hash function SHA-256+256 differently:

$$\text{SHA-256+256}(x) = \text{SHA-256}(0||x) \; || \; \text{SHA-256}(1||x).$$

What is the collision resistance of (this new) SHA-256+256?

- A 64 bits
- B 128 bits
- C 192 bits
- D 256 bits
- E 384 bits
- F 512 bits

The correct answer is **D** here. After processing 0 or 1, the chaining values diverge and should behave independently. We can picture the two invocations as independent hash function invocations. There is no bottleneck of CV like in the previous example, so both the CV size and the output size are 512 bits.

MD4, MD5, SHA-1

What is the status of these hash functions w.r.t. collision resistance?

- A SHA-1 is theoretically broken, but not MD4 nor MD5
- B MD5 and SHA-1 are theoretically broken, but not MD4
- C MD4, MD5 and SHA-1 are theoretically broken
- D MD4, MD5 and SHA-1 are practically broken

MD4, MD5, SHA-1

What is the status of these hash functions w.r.t. collision resistance?

- A SHA-1 is theoretically broken, but not MD4 nor MD5
- B MD5 and SHA-1 are theoretically broken, but not MD4
- C MD4, MD5 and SHA-1 are theoretically broken
- D MD4, MD5 and SHA-1 are practically broken

The correct answer is **D**. For these three hash functions, there are concrete examples of collisions.

Indifferentiability

Which statement(s) is/are correct?

- A SHA-1 …
- B SHA-256 and SHA-512 …
- C The Merkle-Damgård construction …
- D SHA-3 …
- E The sponge construction …

is/are indifferentiable from a random oracle up to complexity $2^{n/2}$ (A-C) or $2^{c/2}$ (D-E).

Indifferentiability

Which statement(s) is/are correct?

- A SHA-1 ...
- B SHA-256 and SHA-512 ...
- C The Merkle-Damgård construction ...
- D SHA-3 ...
- E The sponge construction ...

is/are indifferentiable from a random oracle up to complexity $2^{n/2}$ (A-C) or $2^{c/2}$ (D-E).

The only correct statement is **E**. Only the mode can be proven indifferentiable. And Merkle-Damgård is not indifferentiable due to the length extension weakness.

KECCAK inverse

When inverting KECCAK, which step is the most costly one?

A θ

B ρ

C π

D χ

E ι

F None of the above

Keccak inverse

When inverting Keccak, which step is the most costly one?

- A θ
- B ρ
- C π
- D χ
- E ι
- F None of the above

The correct answer is **F**. The question was tricky on purpose: There is no Keccak inverse, and the inverse permutation is never invoked in a sponge. Nevertheless, Keccak-f^{-1} exists and in general θ is the most costly step to invert.

Web of trust

I have the following public keys:

- $\mathrm{PK}_{\mathrm{Xavier}}$ checked and signed by me
- $\mathrm{PK}_{\mathrm{Yves}}$ and $\mathrm{Sign}_{\mathrm{SK}_{\mathrm{Xavier}}}(\mathrm{Yves}, \mathrm{PK}_{\mathrm{Yves}})$
- $\mathrm{PK}_{\mathrm{Zoë}}$ and $\mathrm{Sign}_{\mathrm{SK}_{\mathrm{Yves}}}(\mathrm{Zoë}, \mathrm{PK}_{\mathrm{Zoë}})$

Who do I have to trust so that can I trust Zoë's public key?

A Xavier only

B Yves only

C Both Xavier and Yves

Web of trust

I have the following public keys:

- $\mathrm{PK}_{\mathrm{Xavier}}$ checked and signed by me
- $\mathrm{PK}_{\mathrm{Yves}}$ and $\mathrm{Sign}_{\mathrm{SK}_{\mathrm{Xavier}}}(\mathrm{Yves}, \mathrm{PK}_{\mathrm{Yves}})$
- $\mathrm{PK}_{\mathrm{Zoë}}$ and $\mathrm{Sign}_{\mathrm{SK}_{\mathrm{Yves}}}(\mathrm{Zoë}, \mathrm{PK}_{\mathrm{Zoë}})$

Who do I have to trust so that can I trust Zoë's public key?

A Xavier only

B Yves only

C Both Xavier and Yves

The correct answer is **C**.

If Xavier only, it tells me that I can trust Yves' public key, but not the fact that Yves actually checked Zoë's public key.

If Yves only, nothing tells me that Yves' public key belongs to him, so Yves' signature on Zoë's public key might actually not be from Yves.