Symmetric Key Cryptography

Daniel Mancia

University of Texas at Austin

November 20, 2019

Table of Contents

1. Symmetric Key Cryptography
2. Stream Ciphers
3. Block Ciphers
4. Key Distribution

Table of Contents

1 Symmetric Key Cryptography

2 Stream Ciphers

3 Block Ciphers

4 Key Distribution

What is Symmetric Key Cryptography

- Symmetric key cryptography consists of algorithms that use a shared key for encryption and decryption.

What is Symmetric Key Cryptography

- Symmetric key cryptography consists of algorithms that use a shared key for encryption and decryption.
- There are two types of symmetric key encryption ciphers: Block Ciphers and Stream Ciphers.

What is Symmetric Key Cryptography

- Symmetric key cryptography consists of algorithms that use a shared key for encryption and decryption.
- There are two types of symmetric key encryption ciphers: Block Ciphers and Stream Ciphers.
- For simplicity we are going to assume that there exists a secure communication channel where the two parties can share their key.

Symmetric Key Cryptography

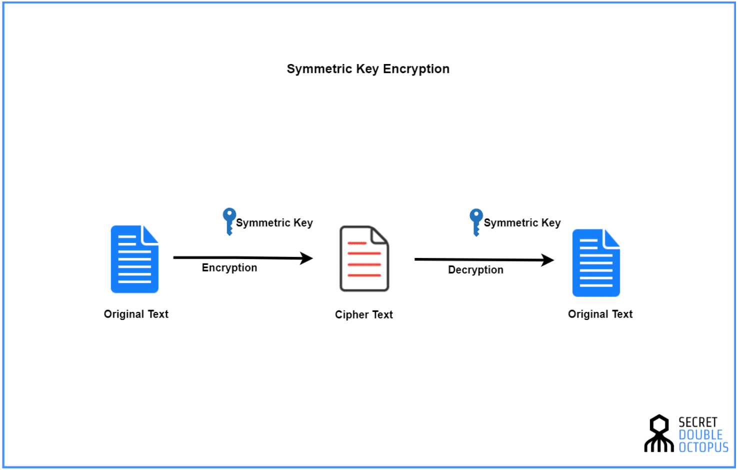

Figure 1: The general idea

Table of Contents

1. Symmetric Key Cryptography
2. Stream Ciphers
3. Block Ciphers
4. Key Distribution

What is a Stream Cipher?

- A stream cipher encrypts the bits of the plaintext with some pseudorandom bit stream called the keystream.

What is a Stream Cipher?

- A stream cipher encrypts the bits of the plaintext with some pseudorandom bit stream called the keystream.
- The keystream is generated from a random seed value.

What is a Stream Cipher?

- A stream cipher encrypts the bits of the plaintext with some pseudorandom bit stream called the keystream.
- The keystream is generated from a random seed value.
- The key is therefore the seed value used to generate the random values.

What is a Stream Cipher?

- A stream cipher encrypts the bits of the plaintext with some pseudorandom bit stream called the keystream.
- The keystream is generated from a random seed value.
- The key is therefore the seed value used to generate the random values.
- More efficient than block ciphers but much easier to mess up security.

RC4

- The most popular stream cipher designed by Ron Rivest in 1987.

RC4

- The most popular stream cipher designed by Ron Rivest in 1987.
- Used in WEP (1987), WPA (2003/2004), SSL (1995), TLS (1999) until it was prohibited in 2015 because of its insecurity.

RC4

- The most popular stream cipher designed by Ron Rivest in 1987.
- Used in WEP (1987), WPA (2003/2004), SSL (1995), TLS (1999) until it was prohibited in 2015 because of its insecurity.

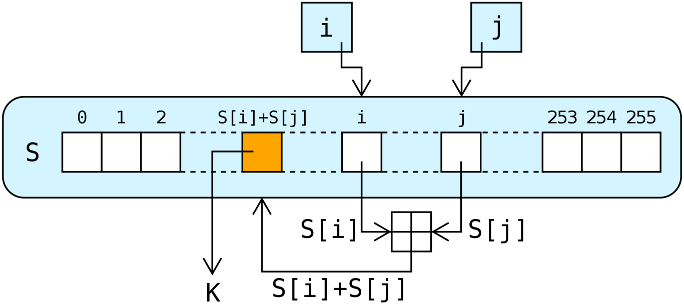

Figure 2: RC4 keystream

Stream Ciphers Attacks

- Keys should have a large period and should not have any subtle biases within them.
- Keys should never be used more than once (Reused Key attack)
- Valid decryption does not imply authenticity (Bit flipping attack).

Table of Contents

1. Symmetric Key Cryptography

2. Stream Ciphers

3. Block Ciphers

4. Key Distribution

Block Ciphers

- A block cipher encrypts a block of bits using a specified key.

Block Ciphers

- A block cipher encrypts a block of bits using a specified key.
- Formally we have the following functions
  1. $E_K(P) := E(K, P) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$
  2. $E_K(C)^{-1} := D_K(C) := D(K, C) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$
  3. $\forall K \quad D_K(E_K(P)) = P$

Block Ciphers

- A block cipher encrypts a block of bits using a specified key.
- Formally we have the following functions
  1. $E_K(P) := E(K, P) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$
  2. $E_K(C)^{-1} := D_K(C) := D(K, C) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$
  3. $\forall K \quad D_K(E_K(P)) = P$
- Famous block ciphers: DES, AES, Blowfish.

AES

- "Advanced Encryption Standard"

AES

- "Advanced Encryption Standard"
- Was adopted by the U.S. government in 2001 and is currently used worldwide.

AES

- "Advanced Encryption Standard"
- Was adopted by the U.S. government in 2001 and is currently used worldwide.
- AES is a substitution–permutation network (AES is annoying to explain, if you want more details on implementation just read the Wikipedia page or the spec).

AES

- "Advanced Encryption Standard"
- Was adopted by the U.S. government in 2001 and is currently used worldwide.
- AES is a substitution–permutation network (AES is annoying to explain, if you want more details on implementation just read the Wikipedia page or the spec).
- AES works on fixed block size of 128 bits and key size of 128, 192, or 256 bits

Modes of Operation

- How can we encrypt arbitrary data if we can only encrypt 128 bits with AES?

Modes of Operation

- How can we encrypt arbitrary data if we can only encrypt 128 bits with AES?
- There are multiple ways but we will only cover ECB and CBC today.

ECB

- The simplest way to encrypt, just do AES on 128 bit chunks of the data.

ECB

- The simplest way to encrypt, just do AES on 128 bit chunks of the data.
- Requires data to be padded.

ECB

- The simplest way to encrypt, just do AES on 128 bit chunks of the data.
- Requires data to be padded.
- Unfortunately the same plaintext blocks will encrypt to the same ciphertext blocks.

ECB

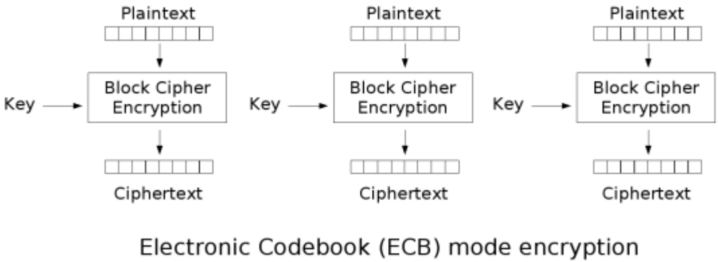

Figure 3: ECB encryption

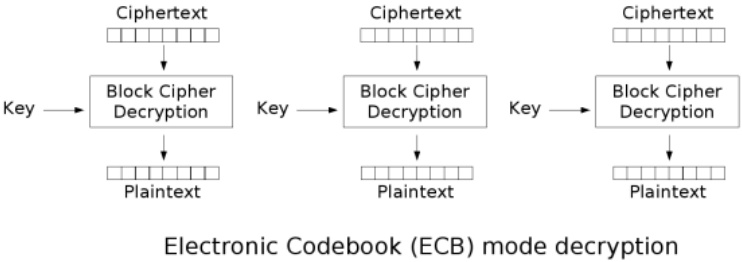

Figure 4: ECB decryption

ECB

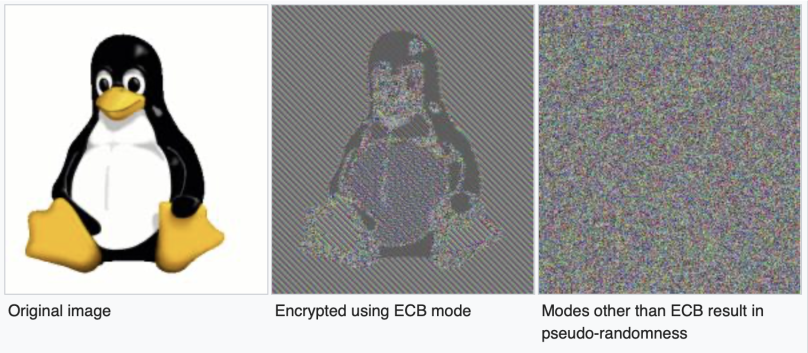

Figure 5: Fatal flaw of ECB

CBC

- Most commonly used mode of operation.

CBC

- Most commonly used mode of operation.
- Requires padding.

CBC

- Most commonly used mode of operation.
- Requires padding.
- Each block of the plaintext is XORed with the previous ciphertext block.

CBC

- Most commonly used mode of operation.
- Requires padding.
- Each block of the plaintext is XORed with the previous ciphertext block.
- What about the first plaintext block???

CBC

- Most commonly used mode of operation.
- Requires padding.
- Each block of the plaintext is XORed with the previous ciphertext block.
- What about the first plaintext block???
- Need to specify an IV (Initialization Vector).

CBC

- Most commonly used mode of operation.
- Requires padding.
- Each block of the plaintext is XORed with the previous ciphertext block.
- What about the first plaintext block???
- Need to specify an IV (Initialization Vector).
- Math formulas:
  - $C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$
  - $P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV$

CBC

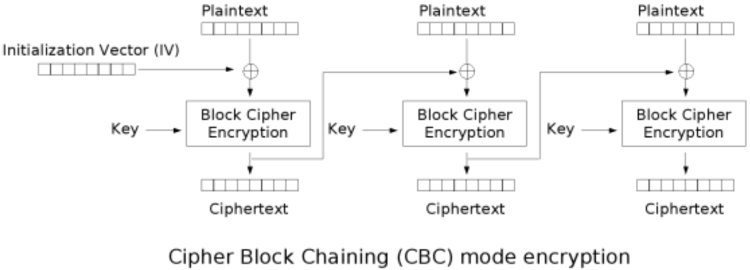

Figure 6: CBC encryption

CBC

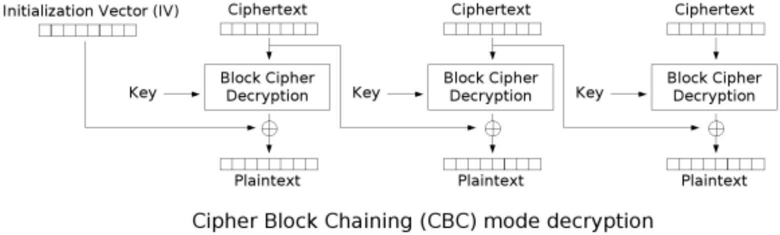

Figure 7: CBC Decryption

Block Cipher Attacks

- ECB is susceptible to a chosen plaintext attack.
- CBC is susceptible to bit flipping and padding oracle attacks.

Table of Contents

1. Symmetric Key Cryptography
2. Stream Ciphers
3. Block Ciphers
4. Key Distribution

Key Distribution

- What if we don't have access to a completely secure communication channel?

Key Distribution

- What if we don't have access to a completely secure communication channel?
- Need some way to share keys.

Diffie-Hellman

1. Alice and Bob agree on a prime number p.
2. Alice chooses a secret integer a and sends Bob $A = g^a \mod p$.
3. Bob chooses a secret integer b and sends Alice $B = g^b \mod p$.
4. Alice computes $B^a \mod p$ and Bob computes $A^b \mod p$.
5. Notice that Alice and Bob now share the same number because $A^b = B^a = g^{ab} \mod p$.

Diffie-Hellman

1. Alice and Bob agree on a prime number p.
2. Alice chooses a secret integer a and sends Bob $A = g^a \mod p$.
3. Bob chooses a secret integer b and sends Alice $B = g^b \mod p$.
4. Alice computes $B^a \mod p$ and Bob computes $A^b \mod p$.
5. Notice that Alice and Bob now share the same number because $A^b = B^a = g^{ab} \mod p$.

- Secret values: a, b
- Public values: g, p, A, B

Diffie-Hellman

- Hardness assumption: Discrete logarithm
- Works the same over Elliptic Curves.