Symmetric Encryption

- CEG 6430/4430 Cyber Network Security
- Junjie Zhang
- junjie.zhang@wright.edu
- Wright State University

Encryption and Decryption

- plaintext: m
- secret: k
- ciphertext: c
- encryption: $c = enc(m, k_{enc})$
- decryption: $m = dec(c, k_{dec})$

Symmetric and Asymmetric Encryption

Symmetric Encryption

- Use the same key for both encryption and decryption.
- $k_{enc} == k_{dec}$

Asymmetric Encryption

- Use different keys for both encryption and decryption.
- $k_{enc} \neq k_{dec}$

Public Key and Private Key

Asymmetric Encryption:

$$c = enc(m, s)$$
$$m = dec(c, k)$$

(s, k) forms a public-private key pair. One is kept as secret and another one is shared with the public.

Some Algorithms

Symmetric Encryption

- Block Cipher: DES, 3DES, AES
- Stream Cipher: RC4

Asymmetric Encryption

- RSA
- Diffie-Hellman, ECDSA, ECDH (More likely to be considered as *key exchange algorithms* however)

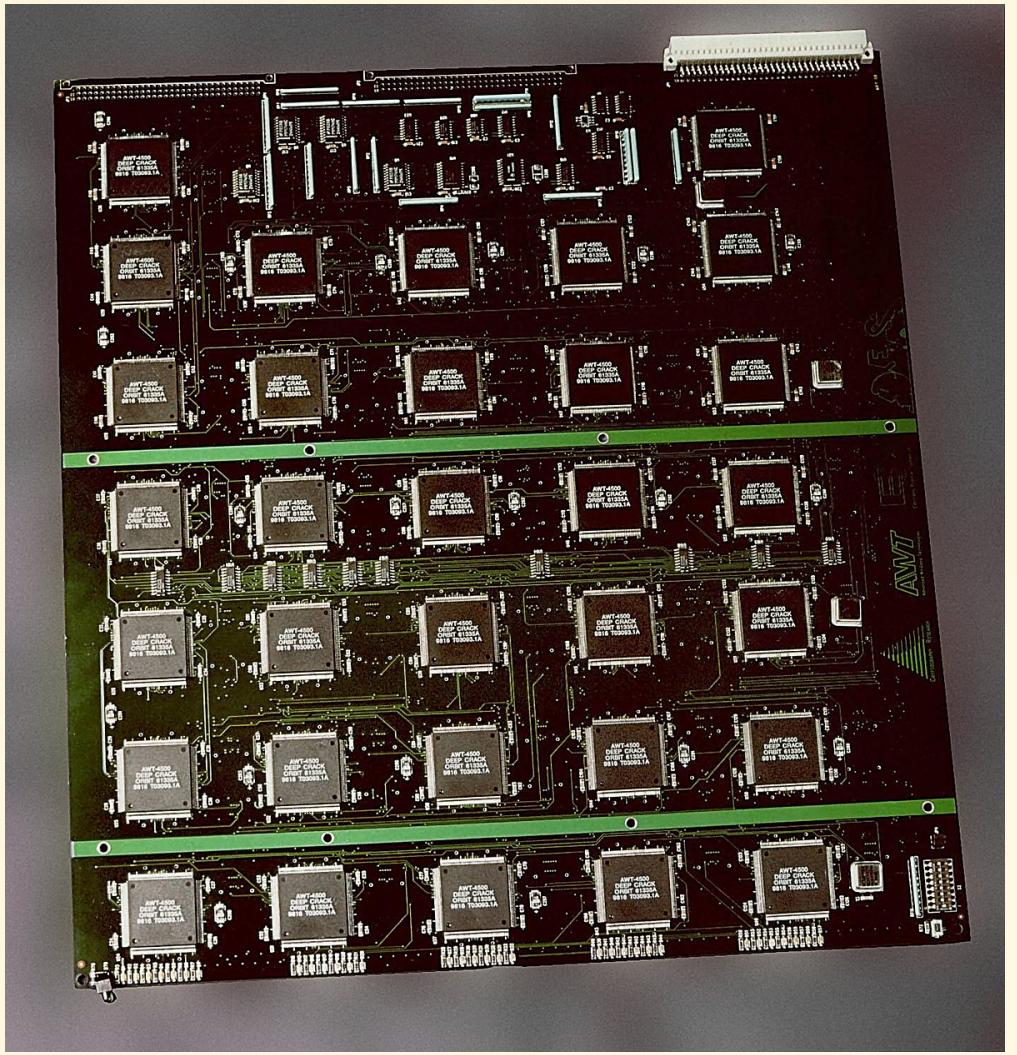
DES

Data Encryption Standard (DES)

- A symmetric-key-based block cipher
  - Block Size (64 bits)
  - Key size (56 bits)
- Designed by IBM
- US national standard from 1977 to 2001
- *A Feistel network with 16 rounds*

3DES

- 56 bits of keys are insufficient.
- 3DES increases the security to about 112 bits.
  - C = $E(E(E(M, k_1), k_2), k_3)$
  - M = $D(D(D(C, k_3), k_2), k_1)$
- Why not 2DES?
  - Meet-in-the-middle attack.



Advanced Encryption Standard (AES)

Comparing DES and AES

	DES	AES
Developed	1977	2000
Key Length	56 bits	128, 192, or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128 bits
Security	Proven inadequate	Considered secure

Questions

DES Block Size: 64 Bits
AES Block Size: 128 Bits

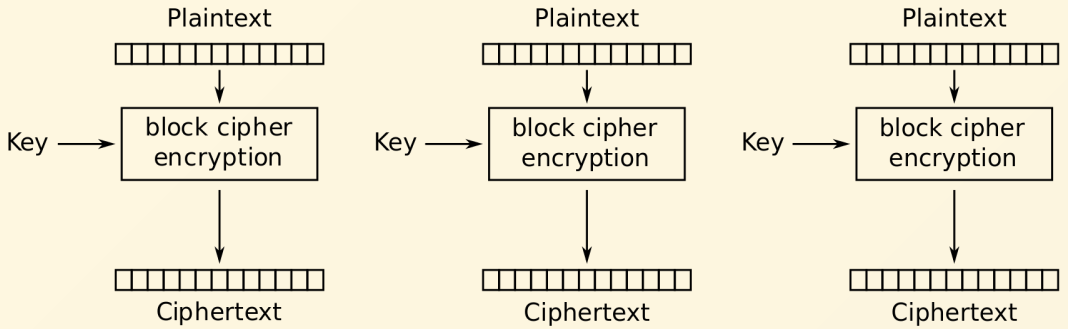
- What if I have less data to be encrypted?
  - Padding
- What if I have more data to be encrypted?
  - Modes of Operations

Modes of Operations

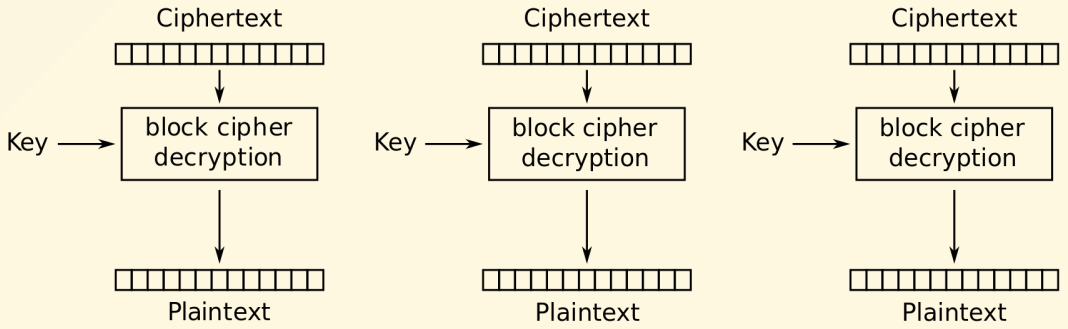
To encrypt and decrypt data with size greater than that of a block cipher.

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter (CTR)

Electronic Codebook (ECB)



Electronic Codebook (ECB) mode encryption

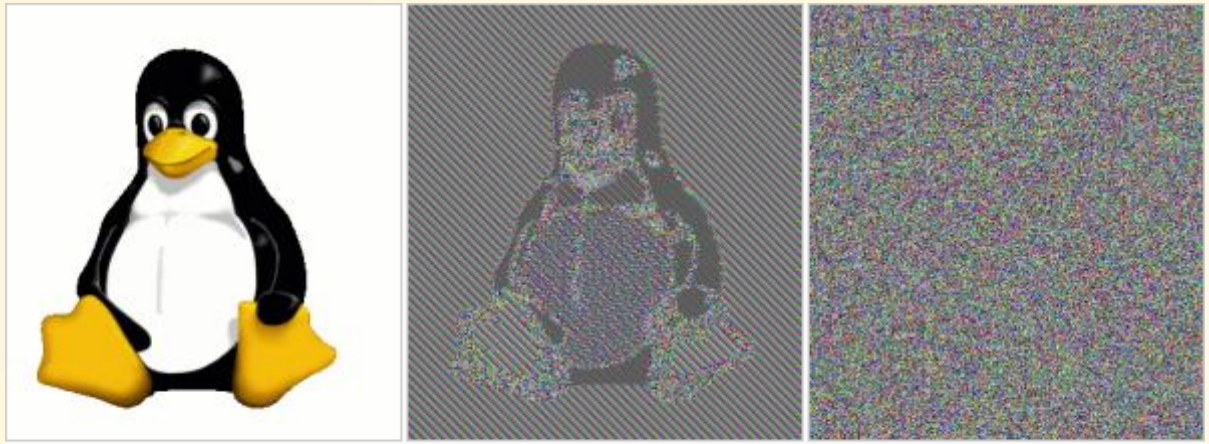


Electronic Codebook (ECB) mode decryption

Electronic Codebook (ECB)

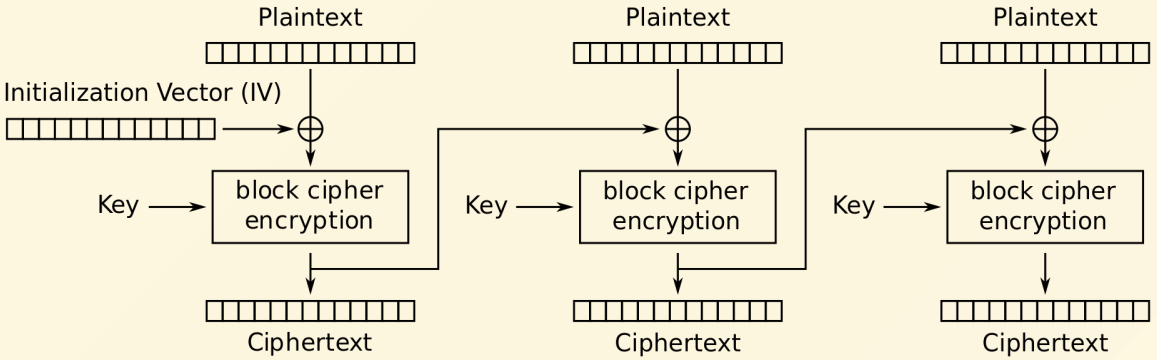
It does not hide data patterns well.

- If two blocks are the same, their ciphertexts are the same.

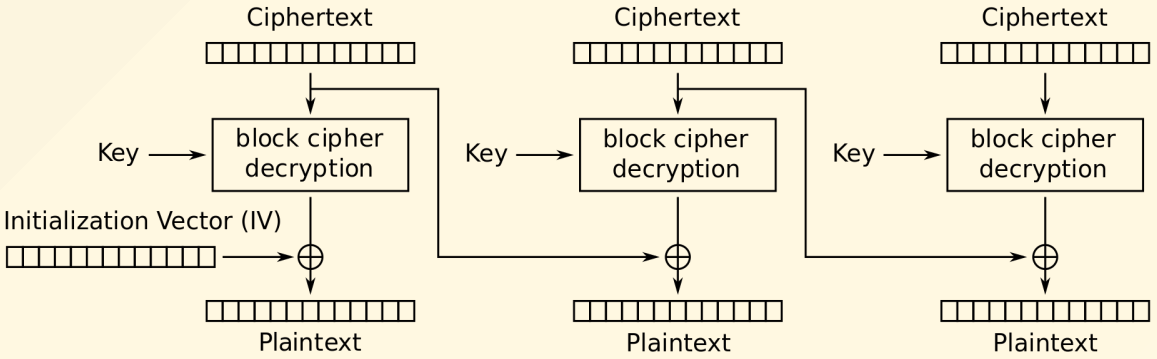


Original image | Encrypted using ECB mode | Modes other than ECB result in pseudo-randomness

Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

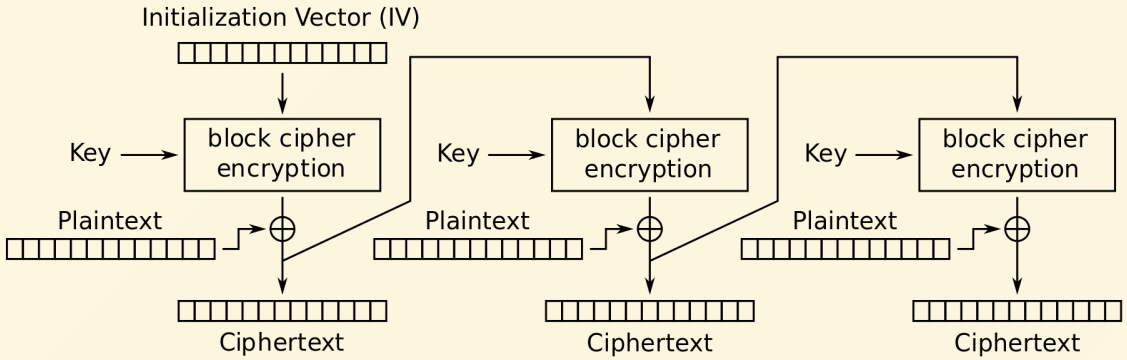


Cipher Block Chaining (CBC) mode decryption

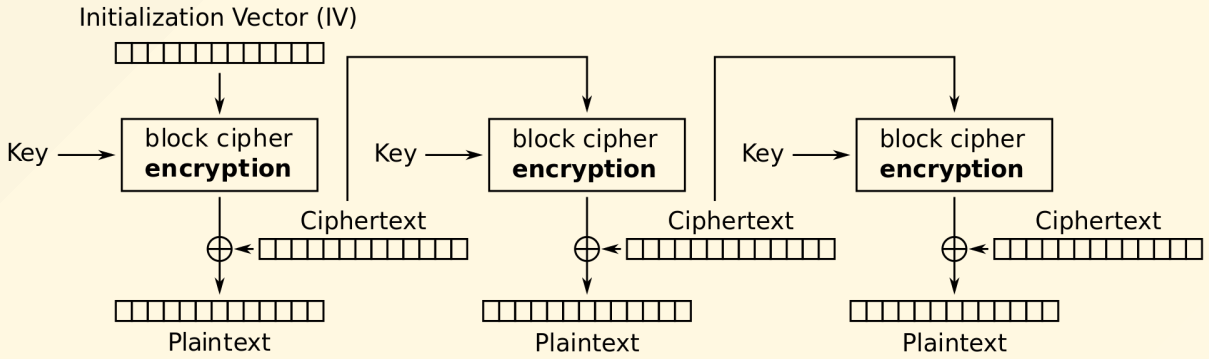
Cipher Block Chaining (CBC)

- Most commonly used mode of operation.
- Initialization Vector (IV)
  - sent with ciphertexts.
  - should never be reused.
- Limitations
  - Encryption is sequential - cannot be parallelized. However, decryption can.
  - Messages must be padded - so does ECB.

Full-Block Cipher Feedback (CFB)



Cipher Feedback (CFB) mode encryption

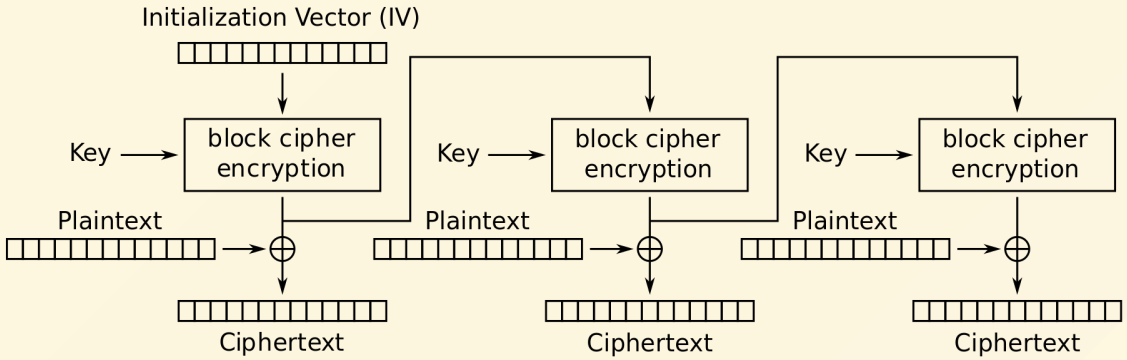


Cipher Feedback (CFB) mode decryption

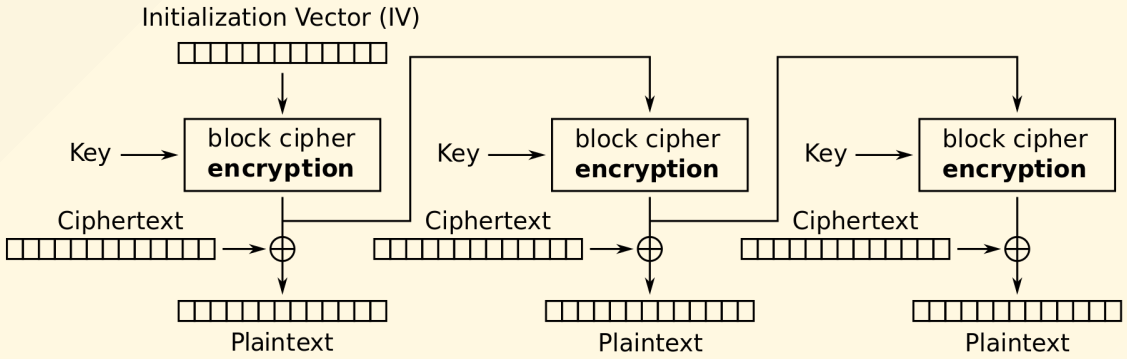
Full-Block Cipher Feedback (CFB)

- Similar to CBC
  - encryption cannot be parallelized, but the decryption can.
  - IV can be sent and visible to the attacker.
  - IV should not be reused.
- You do **not** need the **decryption** part of the block cipher.
- No need to **pad** the (last) message.

Output Feedback (OFB)



Output Feedback (OFB) mode encryption

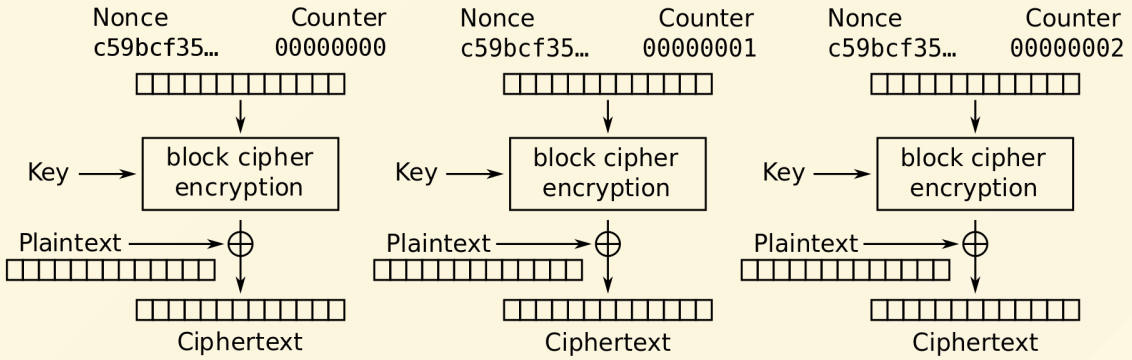


Output Feedback (OFB) mode decryption

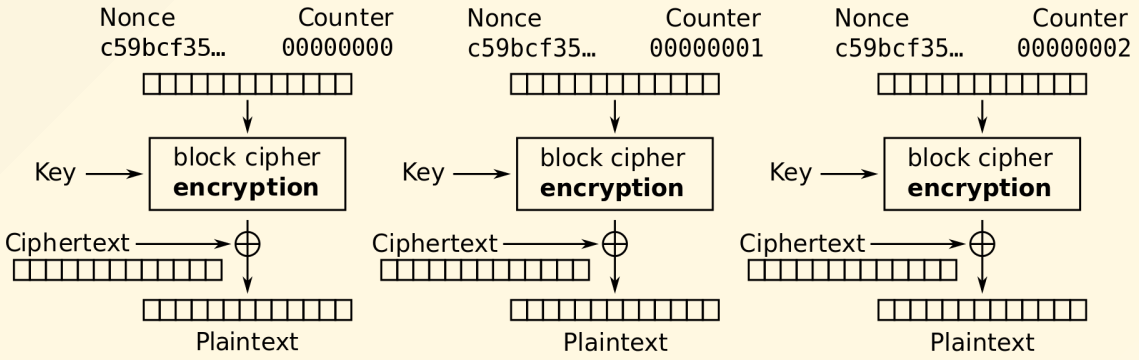
Output Feedback (OFB)

- You do **not** need the **decryption** part of the block cipher.
- No need to **pad** the (last) message.
- You cannot do either encryption or decryption in parallel.
  However, you can pre-calculate the encryption outputs if you know the IV.
- Again, IV
  - IV can be sent and visible to the attacker.
  - IV should not be reused.

Counter (CTR)



Counter (CTR) mode encryption



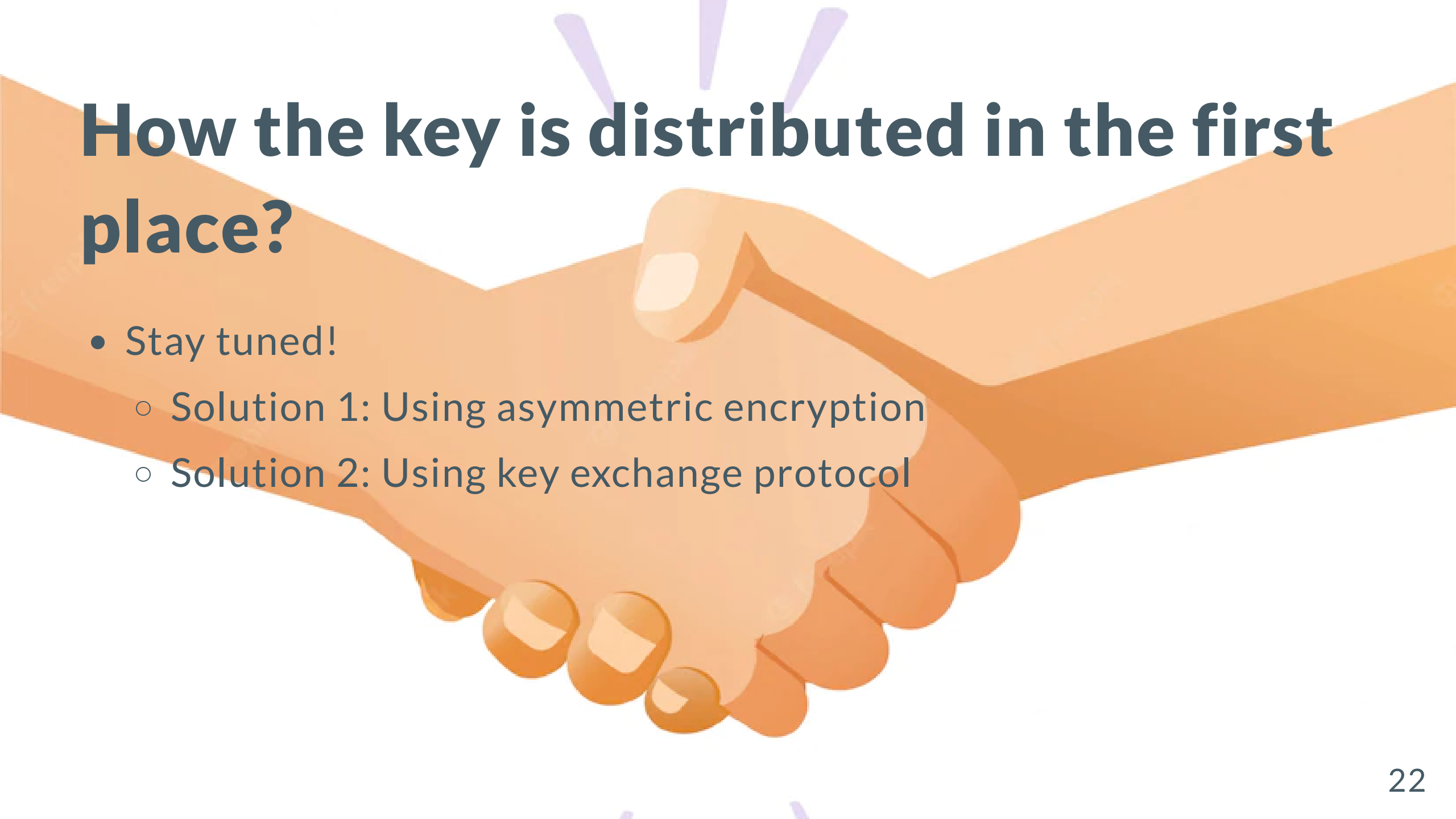
Counter (CTR) mode decryption

Counter (CTR)

- You do **not** need the **decryption** part of the block cipher.
- No need to **pad** the (last) message.
- You can~~not~~ do ~~either~~ both encryption ~~or~~ and decryption in parallel. ~~However, you can pre-calculate the encryption outputs if you know the IV.~~
- Again, ~~IV~~ nonce
  - ~~IV~~ nonce can be sent and visible to the attacker.
  - ~~IV~~ nonce should not be reused.

All Done?

How the key is distributed in the first place?



- Stay tuned!
  - Solution 1: Using asymmetric encryption
  - Solution 2: Using key exchange protocol