ECE 443/518 – Computer Cyber Security
Lecture 04 Block Ciphers, Modes of Operation

Professor Jia Wang
Department of Electrical and Computer Engineering
Illinois Institute of Technology

August 28, 2024

Outline

Block Ciphers

DES and AES

Modes of Operation

Reading Assignment

- This lecture: UC 3, 4 except 4.3, 5.1 – 5.1.5
- Next lecture (9/4): Go Introdcution
  - Please install VSCode and Go following the instructions on: `https://docs.microsoft.com/en-us/azure/developer/go/configure-visual-studio-code`

Outline

Block Ciphers

DES and AES

Modes of Operation

Overview

- Substitution cipher $\rightarrow$ OTP (resist brute-force attack, unconditional security) $\rightarrow$ Stream ciphers (CSPRNG)
- How about cryptanalysis based on statistics?
- Simple substitution cipher maps letters to letters.
  - If there is only 26 letters, collecting a few thousands letters (e.g. allow each letter to appear 100 times on average) of ciphertext will reveal substantial amount of statistics.
- For plaintext and ciphertext as bytes, need a few tens of thousand of bytes so each byte appear 100 times on average.
- What about substition on larger blocks of bits?
  - E.g. 64-bit blocks: every block appears once on average in $2^{64} * 8$ bytes – seems longer than any practical message.
  - Need to study more to be a secure cipher.

Block Ciphers

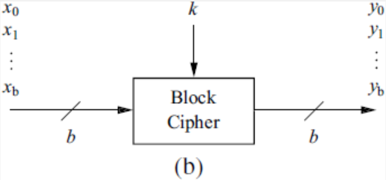


Fig.2 (Paar and Pelzl)

- Shared secret key k.
- Plaintext x as bit blocks of fixed size.
- Each block is encrypted via a block cipher and then concatenated into the ciphertext y.

Discussions

- We first focus on block encryption and decryption, i.e. both x and y are fixed-length bit strings.
  - Popular block lengths in bit: 64, 128, 256, ...
- A substitution cipher with 64-bit blocks need $(2^{64})!$ keys.
  - Generate random permutations if keys are chosen uniformly.
  - But not practical to store or transmit such keys.
- A block cipher only supports a subset of the permutations.
  - Not a concern as long as its key space is large enough, and the permutations "look" random.
  - Key space depends on key sizes: 64-bit, 128-bit, ...
- Additional issues.
  - Modes of operation: how to use information from a previous block when encrypting the next block?
  - Padding: what if plaintext length is not multiples of block size?

Outline

Block Ciphers

DES and AES

Modes of Operation

History of Data Encryption Standard (DES)

- 1972: NBS (now NIST) request for proposals for a standardized cipher in the USA
  - Motivated by demands for encryption in commercial applications.
  - Before this, cryptography and cryptanalysis are considered so crucial for national security that it had to be kept secret.
- 1974: proposal from IBM received
- 1977: NBS release Data Encryption Standard (FIPS PUB 46)
  - IBM cipher modified by NSA.
- 1990's: key space too small (2^{56}) to resist brute-force attack
  - Moore's law: computers become much more powerful
  - Triple DES proposed as a remedy
- 2001: NIST publish Advanced Encryption Standard (AES)
  - This is what you should use instead of DES as of now.

History of Advanced Encryption Standard (AES)

- 1997: NIST call for proposals
  - 128-bit block with 128, 192, and 256 bits keys
  - Efficiency in software and hardware
  - Open selection process
- 1998: 15 candidate algorithms, from several countries
- 1999: 5 finalist algorithms
  - Mars, RC6, Rijndael, Serpent, Twofish
- 2000: Rijndael announced as the winner
- 2001: Advanced Encryption Standard (AES) (FIPS PUB 197)
- 2003: NSA announced that it allows AES to encrypt classified documents up to the level SECRET, and up to the TOP SECRET level for 192 or 256-bit keys.

AES Encryption

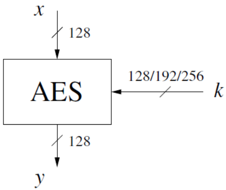


Fig. 4.1 AES input/output parameters

key lengths	# rounds = n_r
128 bit	10
192 bit	12
256 bit	14

Table 4.1

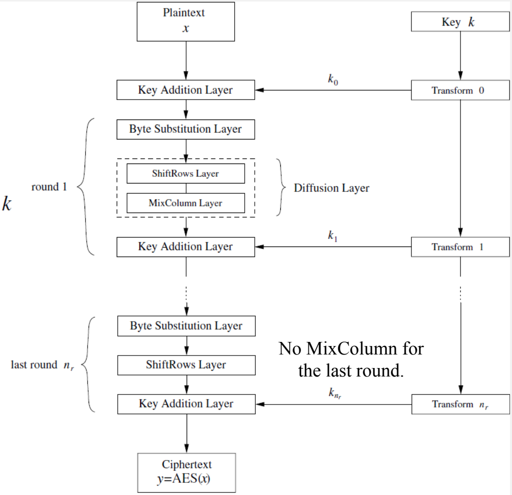


Fig. 4.2 AES encryption block diagram

(Paar and Pelzl)

- Round keys are always 128 bits.

AES Decryption

- Need to invert all layers.
  - Need extra resource though the basic structure is similar.
- Key schedule remains the same.
  - The order to apply subkeys are reversed.

AES Implementations

- A lot of literatures as references.
- Hardware
  - ASIC or FPGA
  - Optimized for throughput, e.g. for 400Gb/s and beyond networking, or power/area, e.g. for IoT devices.
- Software
  - Purely software: table lookup
  - Hardware acceleration: e.g. AES-NI for x86 CPUs
  - Don't implement it by yourself, use a library for correctness, security, and performance.

Outline

Block Ciphers

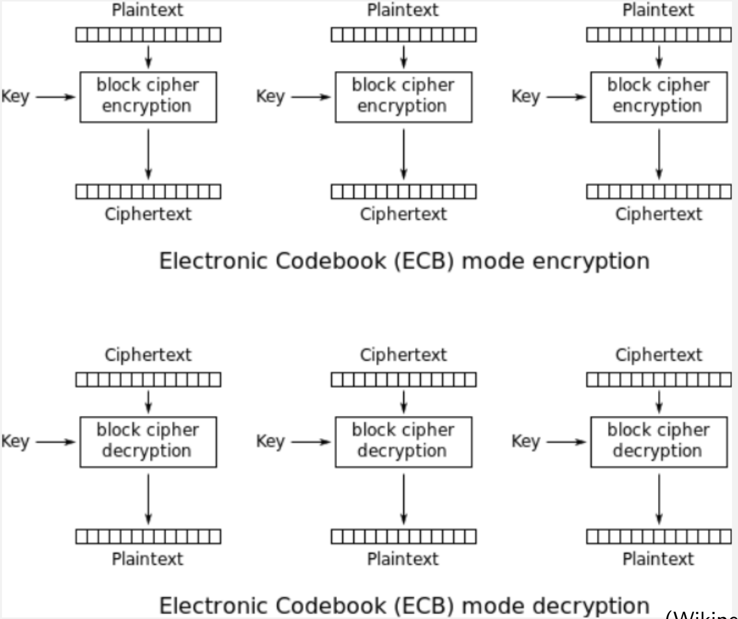
DES and AES

Modes of Operation

Should we apply AES as it is directly to messages?

- What if the message is longer than 128 bits?
- What if the message is not exactly 128 bits?
- Any other concerns?
- What about other block ciphers?

Electronic Code Book (ECB)

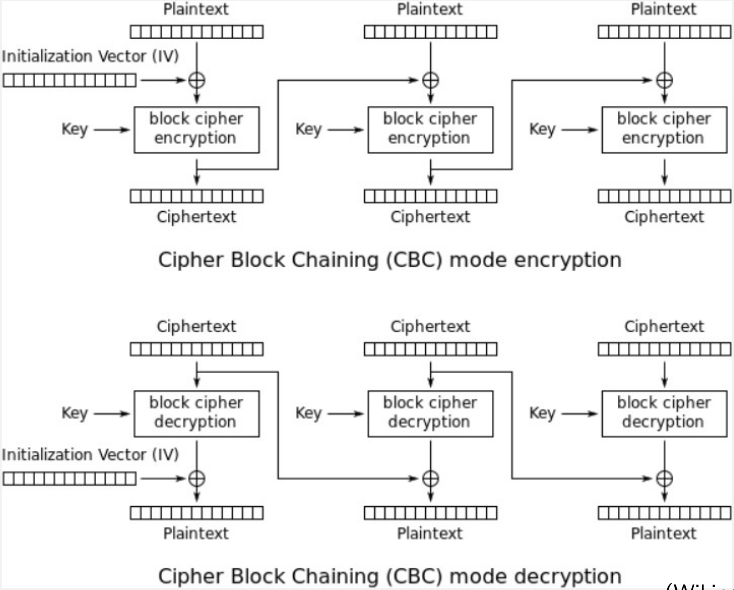


(Wikipedia)

Discussions

- A substitution cipher based on a block cipher like AES.
- Padding: when message size is not multiples of block size
  - Alice appends additional bits that Bob will identify.
  - E.g. 1 followed by necessary number of 0's.
- Oscar the passive adversary
  - Known-plaintext attack using padding.
  - Traffic analysis possible since same plaintext blocks always encrypts to same ciphertext blocks.
- Can be parallelized as long as the message is available.

Cipher Block Chaining (CBC)

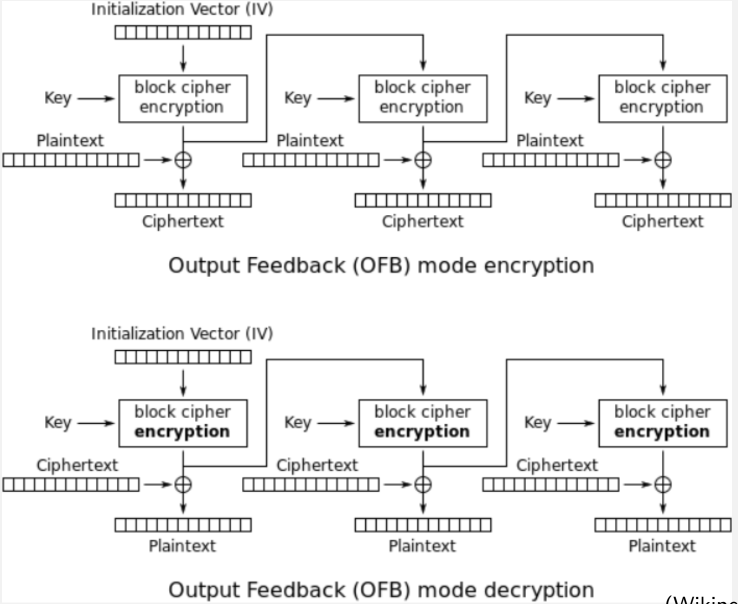


(Wikipedia)

Discussions

- "Randomize" plaintext blocks
  - Use previous ciphertext blocks.
  - Use an initialization vector (IV) for the first plaintext block.
- Choice of IV
  - Probabilistic encryption: different IVs results in different ciphertexts even if the plaintext and the key are the same.
  - A.k.a nonce – a number used only once.
  - Usually randomly chosen and transmitted before ciphertext.
    - Oscar will see it.
    - If that's a concern, Alice could just encrypt IV.
- Only decryption can be parallelized.

Output Feedback (OFB)

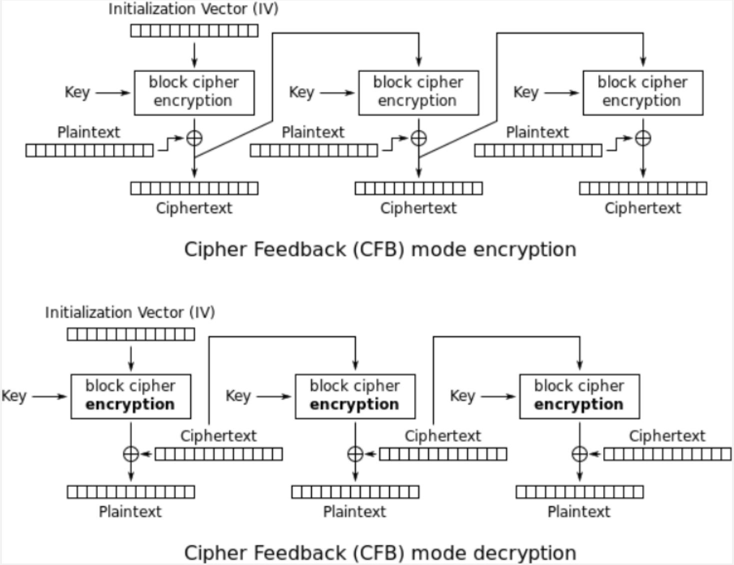


(Wikipedia)

Discussions

- A stream cipher based on a block cipher.
  - Random IV guarantees probabilistic encryption.
  - It is a CSPRNG as long as the block cipher can resist known-plaintext attack.
- Only need encryption from the block cipher.
  - No need to implement decryption – save hardware resource.
- Cannot be parallelized.
  - Key stream can be precomputed as long as storage permits.

Cipher Feedback (CFB)

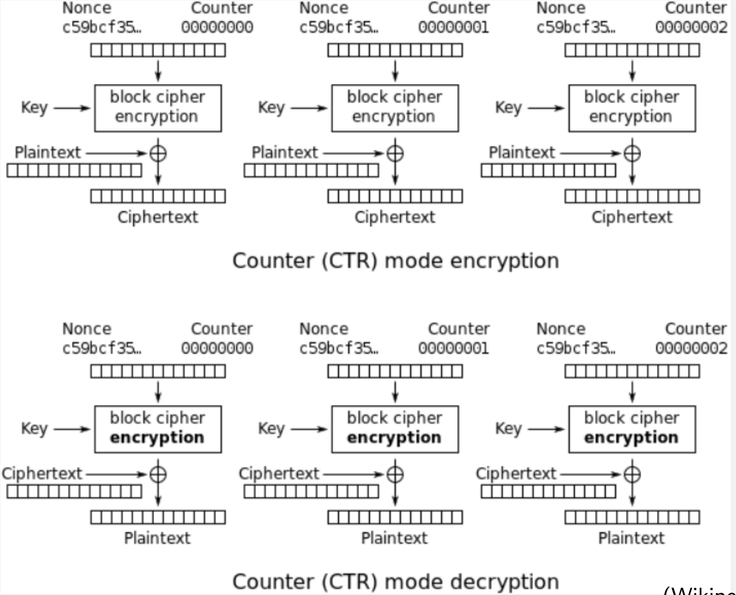


(Wikipedia)

Discussions

- An asynchronous stream cipher as the key stream depends on both key and previou ciphertext (and plaintext).
  - Otherwise very similar to OFB.
- Only need encryption and decryption can be parallelized.

Counter Mode (CTR)



(Wikipedia)

Discussions

- A stream cipher that can be fully parallelized.
- Only need encryption as OFB and CFB.
- There is a limitation on message size for a given IV.
  - OFB also has limitation on message size, although it should be much longer.

Active Adversaries and Integrity

- We introduce passive adversaries to address confidentiality.
- For integrity, we could address it by active adversaries.
  - They can modify or even insert messages.
  - E.g. reorder/substitute/modify/create blocks.
- With the ability to manipulate ciphertext, active adversaries could even
  - Break confidentiality by side-channel attack.
  - Break higher level protocols by replay attack.
- None of the modes of operation can guarantee integrity.
  - No matter how secure the underlying block cipher is.
  - E.g. if reordering and substitution attacks are applied to ECB, all blocks will decrypt correctly but may mean things completely different when combined together.

Summary

- Block ciphers
- DES and AES
- Modes of operation