CRYPTOGRAPHY (CTG)

Diploma in Cybersecurity and Digital Forensics (Dip in CSF)

Academic Year (AY) `21/`22 – Semester 2

WEEK 14.2

ADVANCED ENCRYPTION STANDARD (AES)

Last Updated: 1/11/2020

Contents

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

3

Overview of the AES algorithm

Some Basic Facts

- AES is the most widely used symmetric cipher today
- The algorithm for AES was chosen by the US National Institute of Standards and Technology (NIST) in a multi-year selection process
- The requirements for all AES candidate submissions were:
  - Block cipher with 128-bit block size
  - Three supported key lengths: 128, 192 and 256 bit
  - Security relative to other submitted algorithms
  - Efficiency in software and hardware

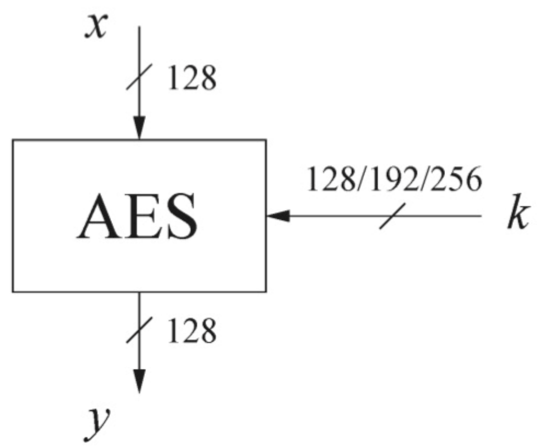
Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Chronology of the AES Selection

- The need for a new block cipher announced by NIST in January, 1997
- 15 candidates algorithms accepted in August, 1998
- 5 finalists announced in August, 1999:
  - Mars – IBM Corporation
  - RC6 – RSA Laboratories
  - Rijndael – J. Daemen & V. Rijmen
  - Serpent – Eli Biham et al.
  - Twofish – B. Schneier et al.
- In October 2000, Rijndael was chosen as the AES
- AES was formally approved as a US federal standard in November 2001

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

AES: Overview



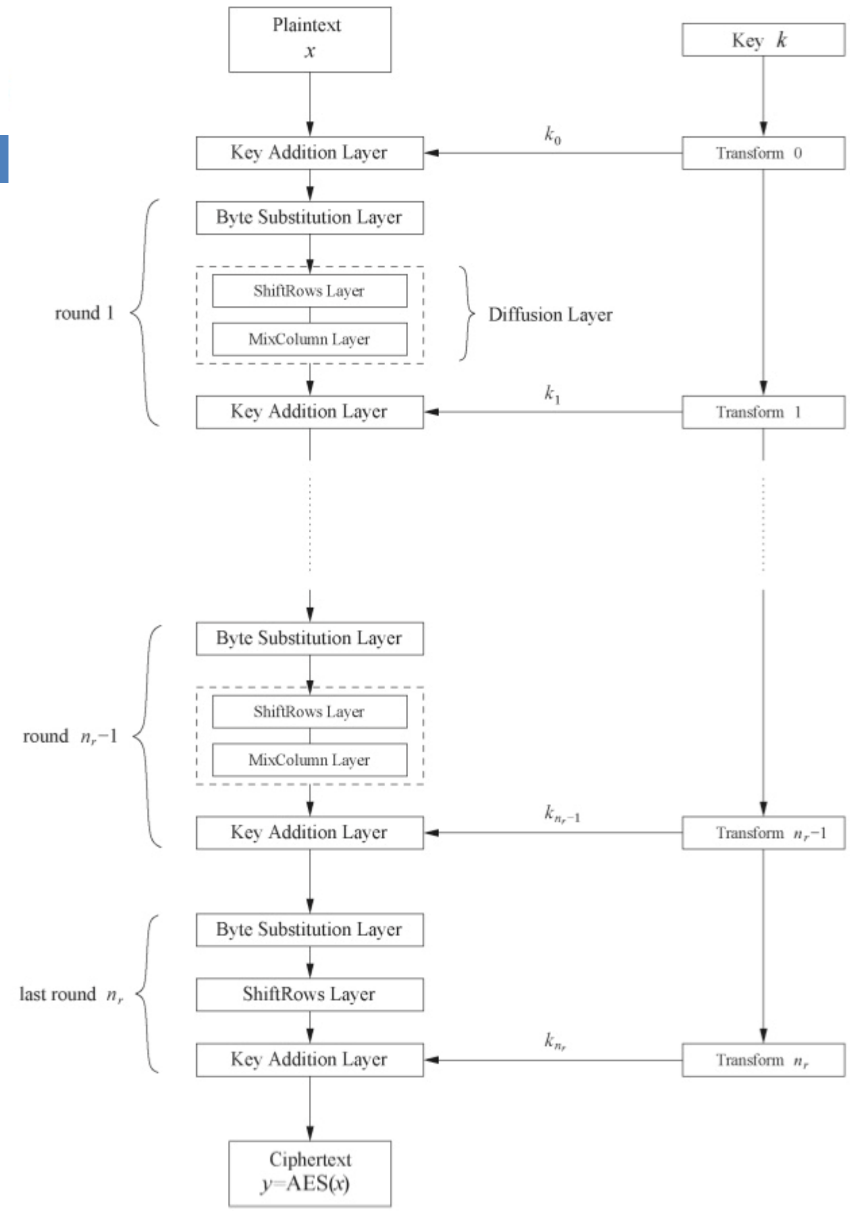
- The number of rounds depends on the chosen key length:

Key length (bits)	Number of rounds
128	10
192	12
256	14

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

AES: Overview

- Iterated cipher with 10/12/14 rounds
- Each round consists of "Layers"



Source: "Understanding Cryptography" by Christof Paar and Jan Pelz

Knowledge Component

High-level description of the AES algorithm

- KeyExpansions
  - round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more (for the initial round).
- InitialRound
  - AddRoundKey—each byte of the state is combined with a block of the round key using bitwise XOR.
- Rounds
  - SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
  - ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
  - MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
  - AddRoundKey
- Final Round (no MixColumns)
  - SubBytes
  - ShiftRows
  - AddRoundKey.

Source: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Internal Structure of AES

Internal Structure of AES

- AES is a byte-oriented cipher
- The state A (i.e., the 128-bit data path) can be arranged in a 4x4 matrix:

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

- with $A_0,\ldots, A_{15}$ denoting the 16-byte input of AES

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Initial Round – Key Addition Layer

- Each byte of the state is combined with a block of the round key using bitwise XOR

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

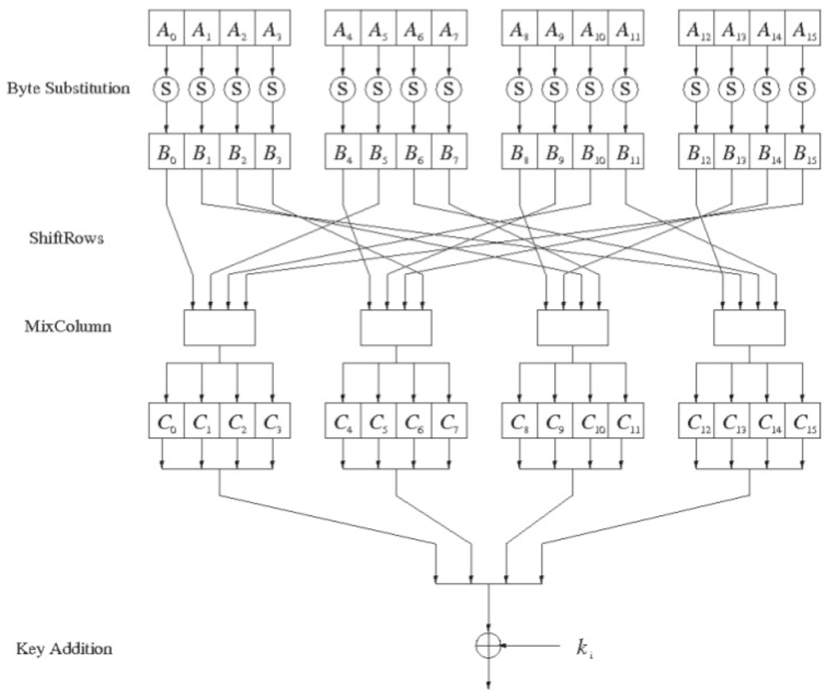
$\oplus$

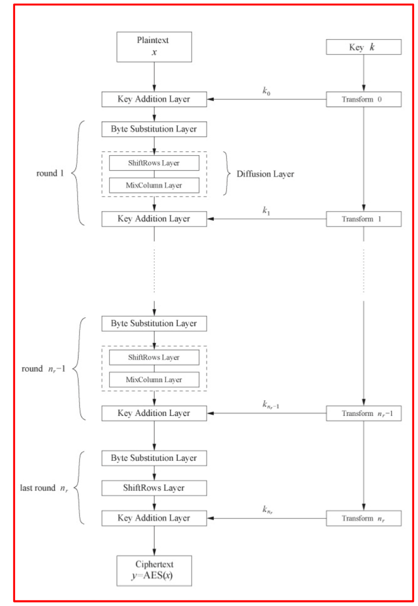
16-byte Round Key 0

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Round Function

- Round function for rounds 1,2,…,n_{r-1}



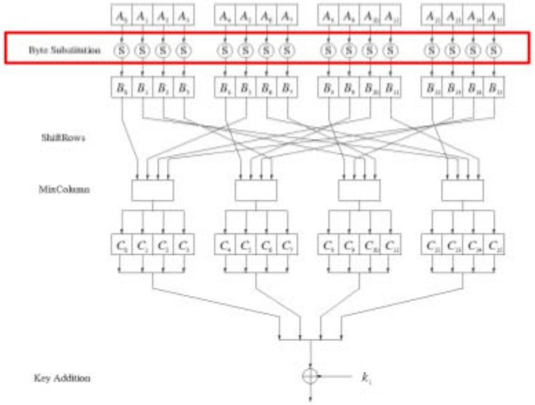


- Note: In the last round, the MixColumn transformation is omitted

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Byte Substitution Layer

Byte Substitution Layer



- The Byte Substitution layer consists of 16 **S-Boxes** with the following properties:

  The S-Boxes are

  - **identical**
  - the only **nonlinear** elements of AES, i.e., ByteSub(A_i) + ByteSub(A_j) $\neq$ ByteSub($A_i + A_j$), for $i,j = 0,\ldots,15$
  - **bijective**, i.e., there exists a one-to-one mapping of input and output bytes

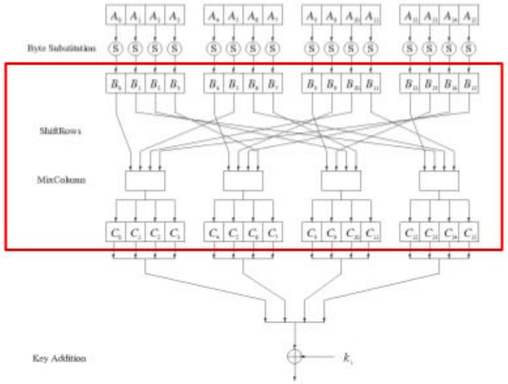
    $\Rightarrow$ S-Box can be uniquely reversed

- In software implementations, the S-Box is usually realized as a lookup table

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Diffusion Layer

Diffusion Layer



The Diffusion layer

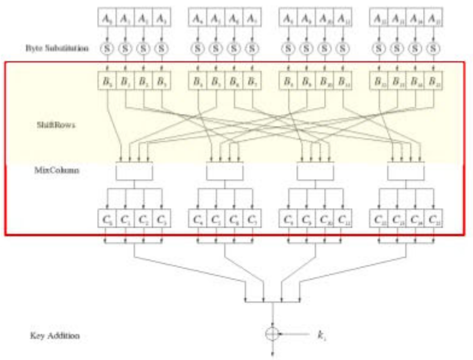
- provides diffusion over all input state bits
- consists of two sublayers:
  - **ShiftRows Sublayer**: Permutation of the data on a byte level
  - **MixColumn Sublayer**: Matrix operation which combines ("mixes") blocks of four bytes
- performs a linear operation on state matrices A, B, i.e.,

$$\mathrm{DIFF}(A) + \mathrm{DIFF}(B) = \mathrm{DIFF}(A + B)$$

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

ShiftRows Sublayer

ShiftRows Sublayer



- Rows of the state matrix are shifted cyclically:

Input matrix

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

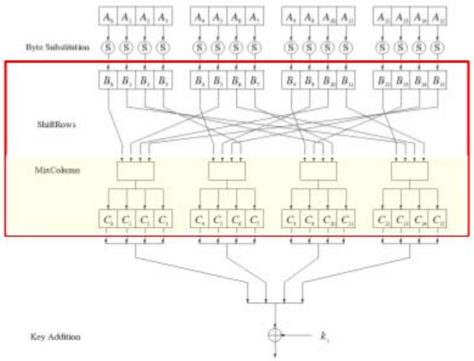
Output matrix

B_0	B_4	B_8	B_{12}	no shift
B_5	B_9	B_{13}	B_1	← one position left shift
B_{10}	B_{14}	B_2	B_6	← two positions left shift
B_{15}	B_3	B_7	B_{11}	← three positions left shift

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

MixColumn Sublayer

MixColumn Sublayer



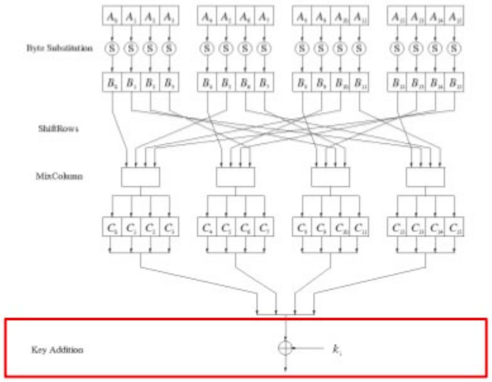
- Linear transformation which mixes each column of the state matrix
- Each 4-byte column is considered as a vector and multiplied by a fixed 4x4 matrix, e.g.,

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

where 01, 02 and 03 are given in hexadecimal notation

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Key Addition Layer



- Inputs:
  - 16-byte state matrix C
  - 16-byte round key k_i
- Output: $C \oplus k_i$
  - $\oplus$: bitwise XOR
  - The round keys are generated in the key schedule

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Key Schedule

- Round keys are derived recursively from the original 128/192/256-bit input key
- Each round has 1 round key, plus 1 round key for the beginning of AES
- Key whitening: Round key is used both at the input and output of AES
  - number of round keys = number of rounds + 1
- There are different key schedules for the different key sizes

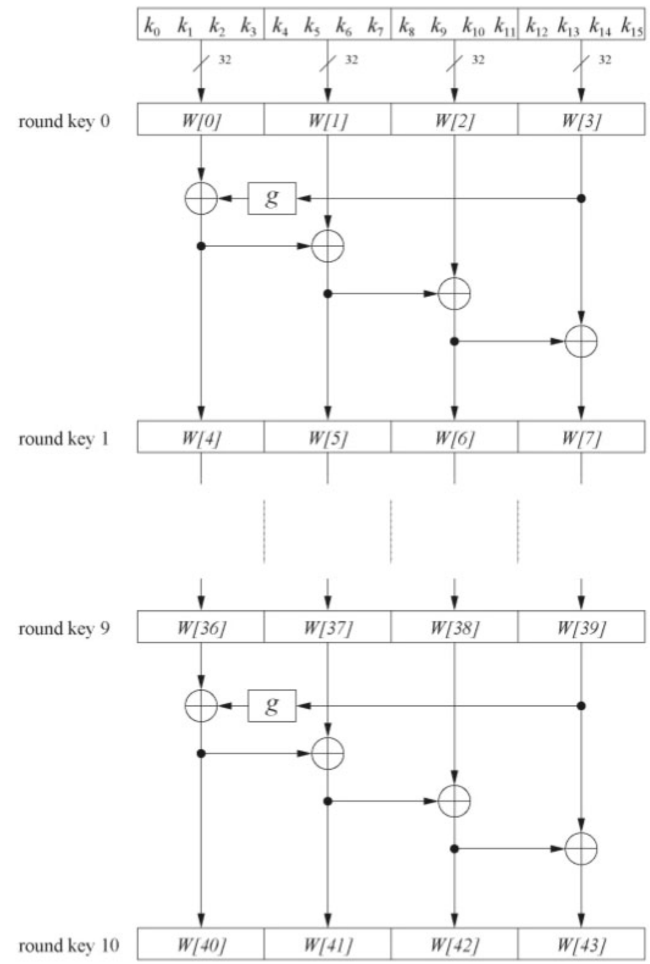
Key length (bits)	Number of rounds	Number of round keys
128	10	11
192	12	13
256	14	15

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Key Schedule

- Word-oriented:
  1 word = 32 bits
- 11 round keys are stored in W[0]...W[3], W[4]...W[7], ... , W[40]...W[43]
- First round key W[0]...W[3] is the original AES key

Example: Key schedule for 128-bit key AES



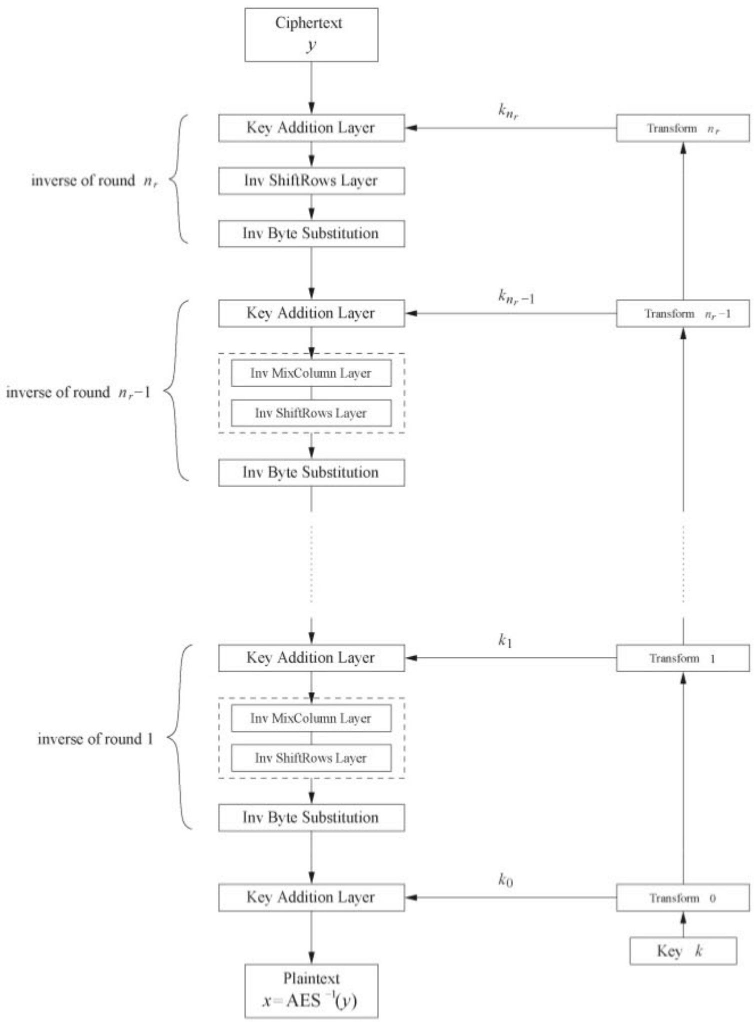
Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

20

Decryption

Knowledge Component

Decryption



- AES is not based on a Feistel network

⇒ All layers must be inverted for decryption:

  - MixColumn layer → **Inv MixColumn layer**
  - ShiftRows layer→ **Inv ShiftRows layer**
  - Byte Substitution layer → **Inv Byte Substitution layer**
  - Key Addition layer is its own inverse

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Decryption key schedule

- Round keys are needed in reversed order (compared to encryption)
- In practice, for encryption and decryption, the same key schedule is used.
  - This requires that all round keys must be computed before the encryption/decryption of the first block can begin

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Security

Security

- **Brute-force attack**
  - Due to the key length of 128, 192 or 256 bits, a brute-force attack is not possible
- **Analytical attacks**
  - There is no analytical attack known that is better than brute-force
- **Side-channel attacks**
  - Several side-channel attacks have been published
  - Note that side-channel attacks do not attack the underlying algorithm but the implementation of it

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

25

Activities

Try out AES

- Excel
  - Download: http://www.nayuki.io/res/aes-cipher-internals-in-excel/aes-cipher-internals.xlsx

- Animation (Rijidael)
  - https://web.archive.org/web/20051124061027/http://www.cs.bc.edu/~straubin/cs381-05/blockciphers/rijndael_ingles2004.swf
  - https://www.youtube.com/watch?v=gP4PqVGudtg

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

27

Summary of AES

Lessons Learned

- AES is a modern block cipher which supports three key lengths of 128, 192 and 256 bit. It provides excellent long-term security against brute-force attacks.
- AES has been studied intensively since the late 1990s and no attacks have been found that are better than brute-force.
- AES is not based on Feistel networks.
- AES provides strong diffusion and confusion.
- AES is part of numerous open standards such as IPsec or TLS, in addition to being the mandatory encryption algorithm for US government applications. It seems likely that the cipher will be the dominant encryption algorithm for many years to come.
- AES is efficient in software and hardware.

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Block Cipher Mode of Operation

Encryption with Block Ciphers

- A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block.
- A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block.

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Encryption with Block Ciphers

- There are several ways of encrypting long plaintexts, e.g., an e-mail or a computer file, with a block cipher ("modes of operation")
  - Electronic Code Book mode (ECB)
  - Cipher Block Chaining mode (CBC) ← Most commonly used
  - Output Feedback mode (OFB)
  - Cipher Feedback mode (CFB)
  - Counter mode (CTR)
  - Galois Counter Mode (GCM)
- All of the 6 modes have one goal:
  - In addition to confidentiality, they provide authenticity and integrity:
    - Is the message really coming from the original sender? (authenticity)
    - Was the ciphertext altered during transmission? (integrity)

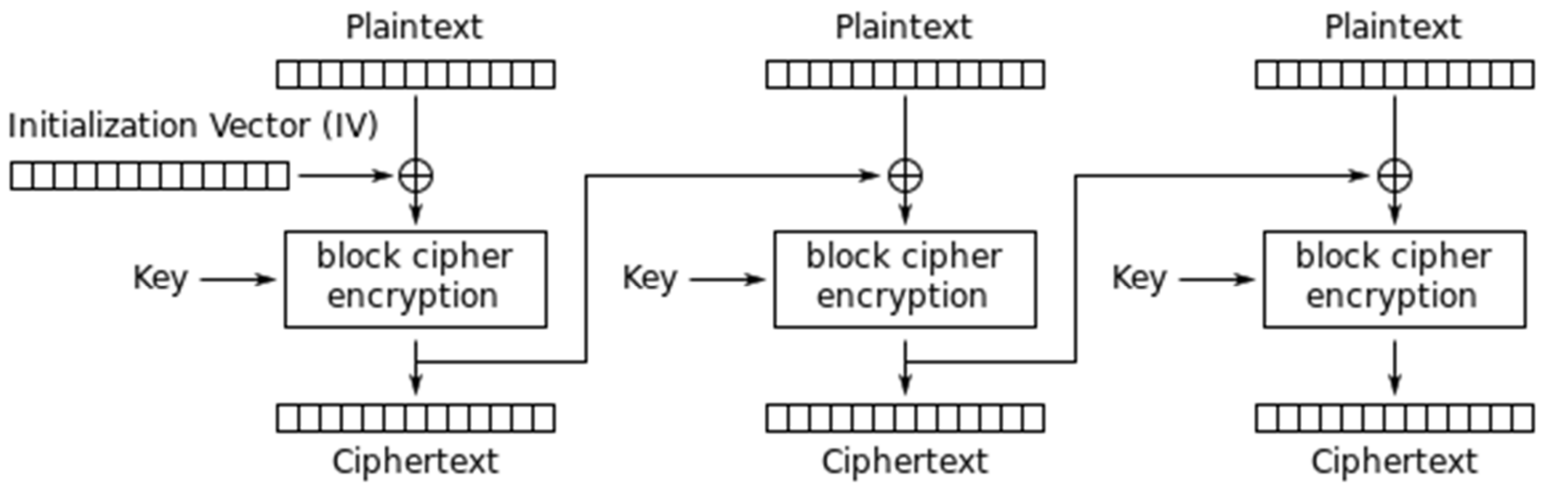
Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Cipher Block Chaining mode (CBC)

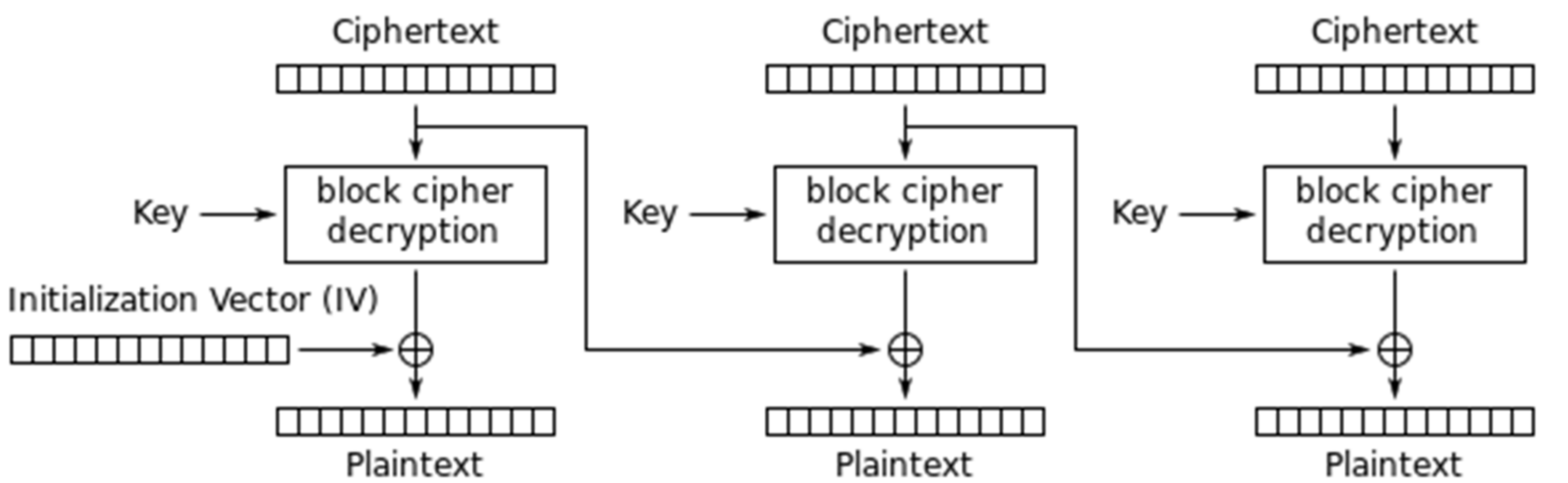
Cipher Block Chaining (CBC)

- IBM invented the Cipher Block Chaining (CBC) mode of operation in 1976.
- In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted.
- This way, each ciphertext block depends on all plaintext blocks processed up to that point.
- To make each message unique, an initialization vector must be used in the first block.

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Initialization vector (IV)

- An initialization vector (IV) is a block of random bits that is used to randomize the encryption and hence to produce distinct ciphertexts even if the same plaintext is encrypted multiple times.
- IV usually does not need to be secret.
- However, in most cases, it is important that an IV is never reused under the same key.
  - For CBC reusing an IV leaks some information about the first block of plaintext.

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Summary of Block Cipher mode of operation

Lessons Learned

- There are many different ways to encrypt with a block cipher.
- Each mode of operation has some advantages and disadvantages.
- In CBC mode, the encryption of all blocks are "chained together" and the encryption is randomized by using an initialization vector (IV)
- An IV is a block of random bits used to randomize the encryption to produce distinct ciphertexts

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl