Module 7

Cryptography

Module Objectives

1. Understanding Cryptographic Techniques
2. Understanding the Different Encryption Algorithms
3. Understanding the Different Hashing Algorithms
4. Overview of Different Cryptography Tools and Hash Calculators
5. Understanding Public Key Infrastructure (PKI)
6. Understanding Digital Signatures and Digital Certificates

Module Flow

01 Discuss Cryptographic Techniques

02 Discuss Various Cryptographic Algorithms

03 Discuss Various Cryptography Tools

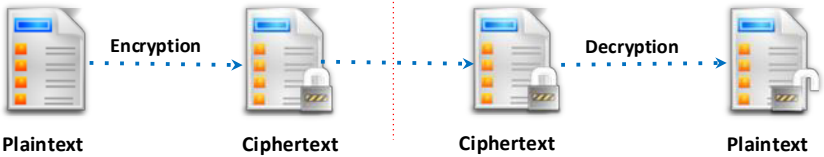
04 Discuss Public Key Infrastructure (PKI)

Cryptography

- Cryptography is the **conversion of data** into a scrambled code that is encrypted and sent across a private or public network
- Cryptography is used to protect confidential data, such as **email messages**, chat sessions, **web transactions**, personal data, **corporate data**, and e-commerce applications

Objectives of Cryptography

- Confidentiality
- Authentication
- Integrity
- Nonrepudiation



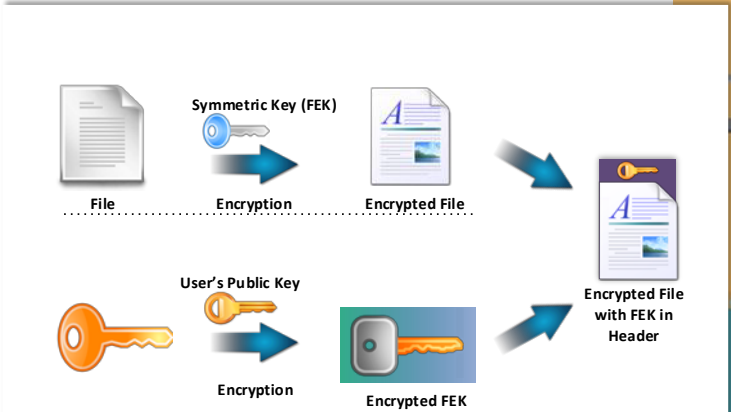
Encryption

- Encryption is a way of **protecting information** by transforming it in such a way that the resulting transformed form is unreadable to an unauthorized party
- To encrypt data, an encryption algorithm uses a **key** to perform a transformation on the data

Types of Encryption

- Symmetric Encryption
- Asymmetric Encryption

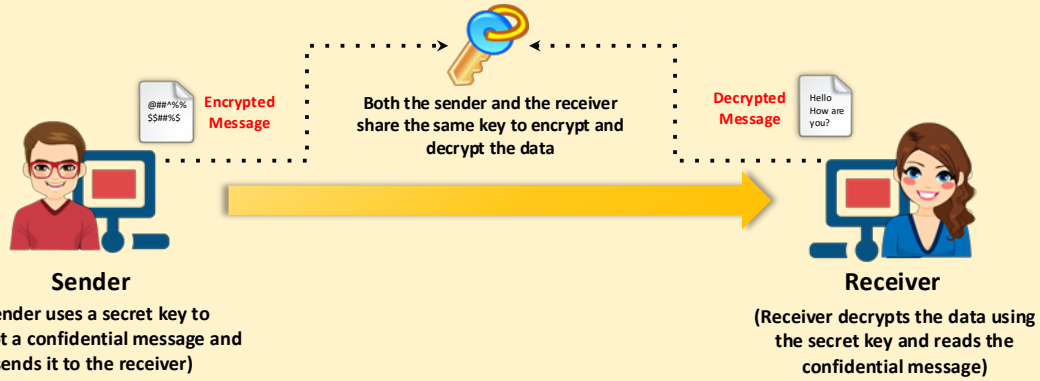
Encryption



Symmetric Encryption

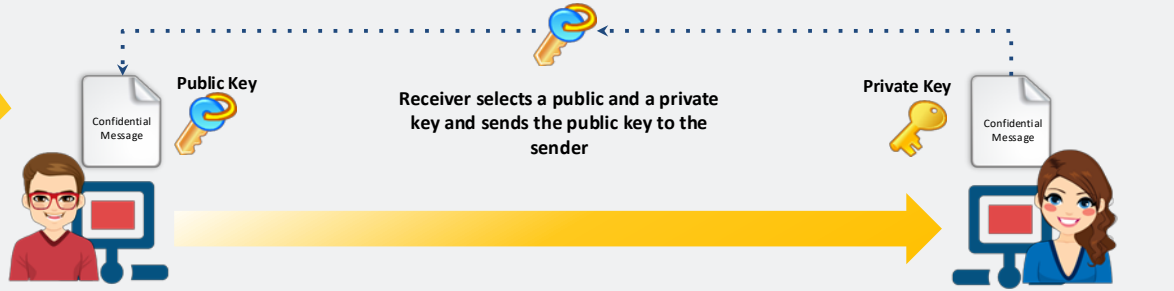
مفتاح واحد
للتشفير

- Symmetric encryption is the oldest cryptographic technique used for **encrypting digital data** in order to **ensure data confidentiality**
- It is called as symmetric encryption since a **single key** is used for encrypting and decrypting the data
- It is used to encrypt **large amounts of data**



Asymmetric Encryption

- Unlike symmetric encryption, asymmetric encryption **uses two separate keys** to carry out encryption and decryption; one key, called the **public key**, is used for encrypting messages, whereas the second key, called the **private key**, is used for decrypting messages
- It is also called **public key encryption** and is used to **encrypt small amounts of data**

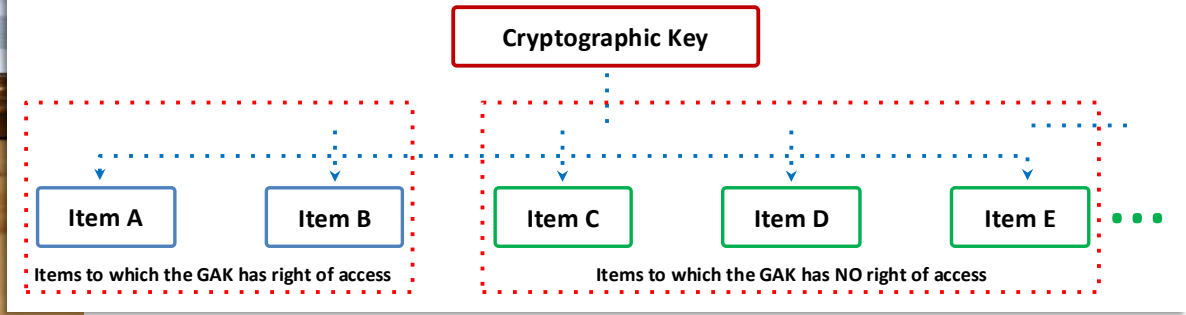


Government Access to Keys (GAK)

GAK means that software companies will give **copies of all keys** (or at least a sufficient proportion of each key that the remainder could be cracked) to the government

The government promises that they will hold on to the keys in a **secure manner** and will only use them when a **court issues a warrant** to do so

To the government, this is similar to the **ability to wiretapping phones**



Module Flow

01 Discuss Cryptographic Techniques

02 Discuss Various Cryptographic Algorithms

03 Discuss Various Cryptography Tools

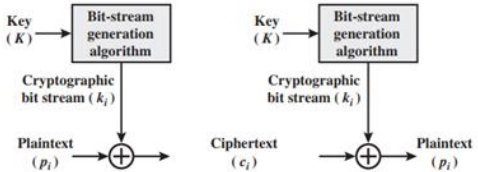
04 Discuss Public Key Infrastructure (PKI)

Ciphers

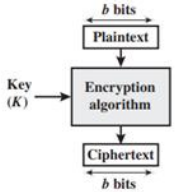
- Types of ciphers
  - Classical Ciphers
    - Substitution cipher
      - A block of plaintext is replaced with ciphertext
    - Transposition cipher
      - The letters of the plaintext are shifted about to form the cryptogram
  - Modern Ciphers
    - Based on the type of key used
      - Private Key
        - Same key is used for encryption and decryption
      - Public Key
        - Two different keys are used for encryption and decryption
    - Based on the type of input data
      - Block Cipher
        - Encrypts blocks of data of fixed size
      - Stream Cipher
        - Encrypts continuous streams of data

Ciphers are algorithms used to encrypt or decrypt the data

Secret Key algorithms



(a) Stream cipher using algorithmic bit-stream generator



(b) Block cipher

Figure 3.1 Stream Cipher and Block Cipher

Secret Key algorithms

- Block ciphers (e.g., DES, AES)
  - takes key and fixed size input block to generate fixed size output block
- Stream ciphers (e.g., RC_4)
  - takes key and generates a stream of pseudorandom bits, XOR'd into data

Data Encryption Standard (DES)

- DES is designed to **encipher** and **decipher** blocks of data consisting of **64 bits** under control of a 56-bit key
- DES is the **archetypal block cipher** — an algorithm that takes a fixed-length string of plaintext bits and transforms it into a ciphertext bit string of the same length
- Due to the **inherent weakness** of DES with today's technologies, some organizations triple repeat the process (3DES) for added strength until they can afford to update their equipment to AES capabilities

About the Algorithm:

Description of the Algorithm The plaintext is 64 bits in length and the key is 56 bits in length; longer plaintext amounts are processed in 64-bit blocks. The DES structure is a minor variation of the Feistel network shown in Figure 2.2. There are 16 rounds of processing. From the original 56-bit key, 16 subkeys are generated, one of which is used for each round.

Strengths of DES measured by considdering two factors:
1.Algorithm itself: concerns raise from the possibility of cryptoanalysis by exploiting DES charactersistics, a lot of studies made on DES but no one discovered a fetal weakness in DES.
2.Key size is a serious concern a 56-but length key which makes brute force attack possible.

A final point: If the only form of attack that could be made on an encryption algorithm is brute force, then the way to counter such attacks is obvious: use longer

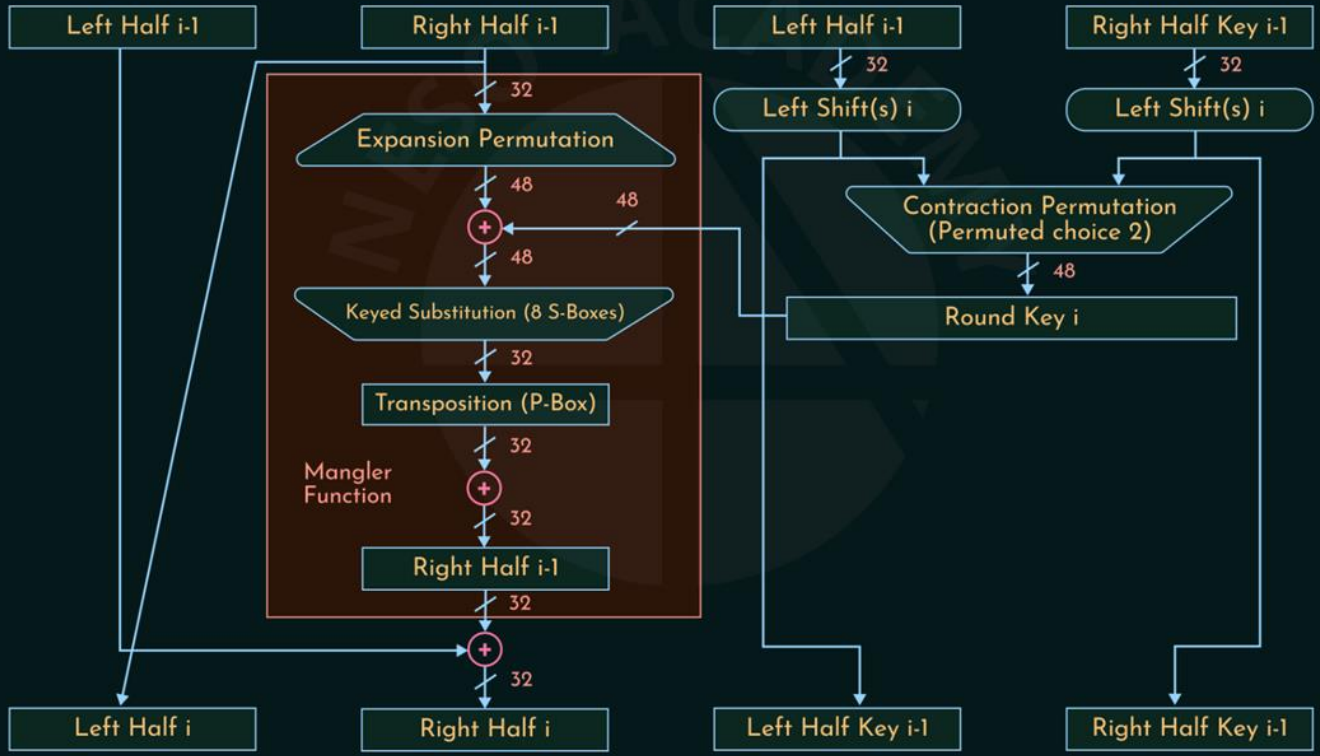
DES Encryption Algorithm

Initial Permutation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

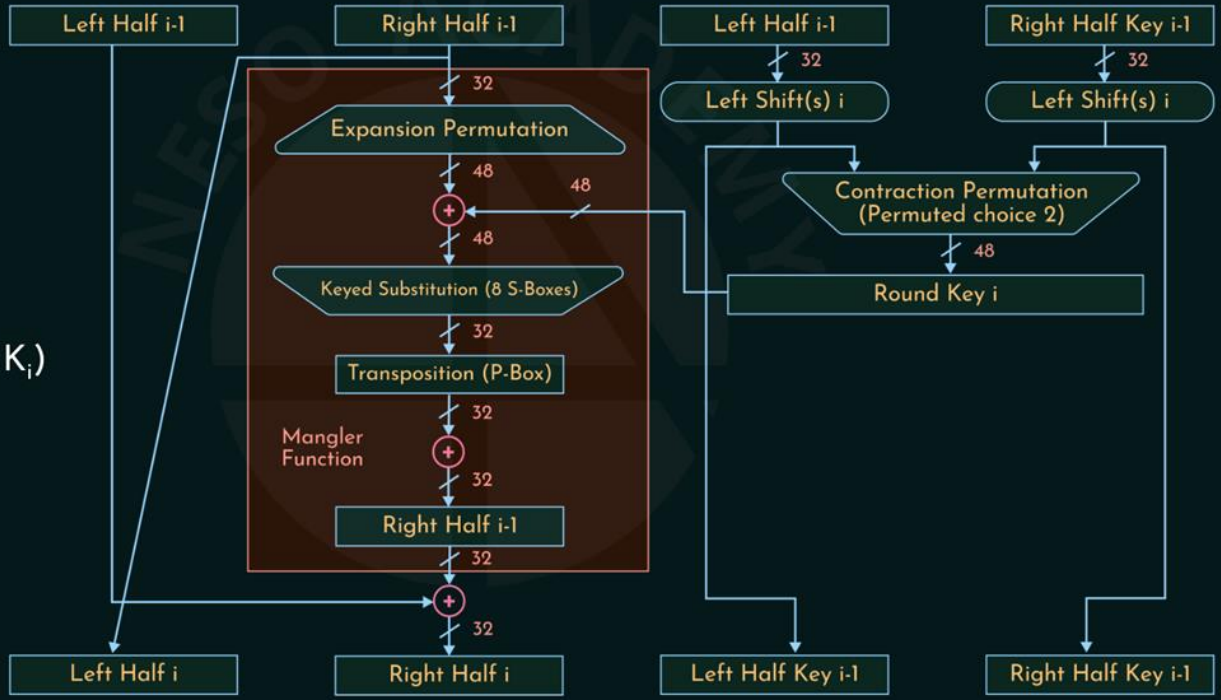
Single Round of DES Algorithm



Single Round of DES Algorithm

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$



Triple DES

With three distinct keys, 3DES has an effective key length of 168 bits, it overcomes the vulnerability to brute-force attack of DEA. And has same cryptoanalsysis resistance as DEA

Advantages:
1.No attack possibel except for brute force attack overcomed by increasing key size
2. If security is the only consideration 3DES is very resistance to cryptoanalysis and it is the appropriate choice.

Limitation:
1. Sluggish in SW: The original DEA was designed for mid-1970s hardware implementation and does not produce efficient software code. 3DES, which has three times as many rounds as DEA, is correspondingly slower.
2. both DEA and 3DES use a 64-bit block size. For reasons of both efficiency and security, a larger block size is desirable.

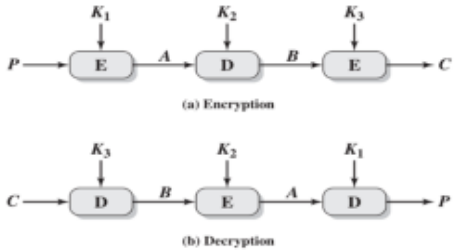


Figure 2.4 Triple DES

C E(K3, D(K2, E(K1, P)))

Advanced Encryption Standard (AES)

- AES is a **symmetric-key** algorithm used by the US government agencies to secure sensitive but unclassified material
- AES is an **iterated block cipher** that works by repeating the same operation **multiple** times
- It has a **128-bit** block size with key sizes of 128, 192, and 256 bits for AES-128, AES-192, and AES-256, respectively

2. The Advanced Encryption Standard (AES)

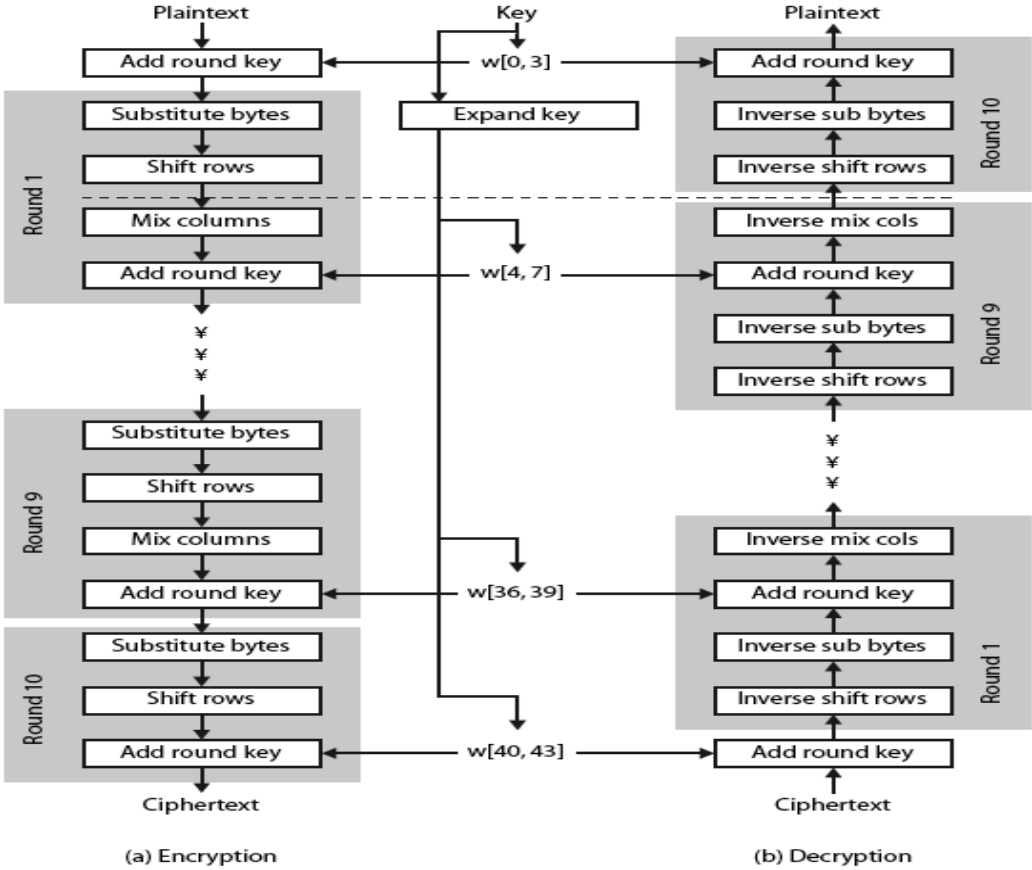
- Triple-DES alternative to DES– but slow, has small blocks
- US NIST issued call for ciphers in 1997
- 15 candidates accepted in Jun 98
- 5 were shortlisted in Aug-99
- Rijndael was selected as the AES in Oct-2000
- issued as FIPS PUB 197 standard in Nov-2001

2.The AES Cipher - Rijndael

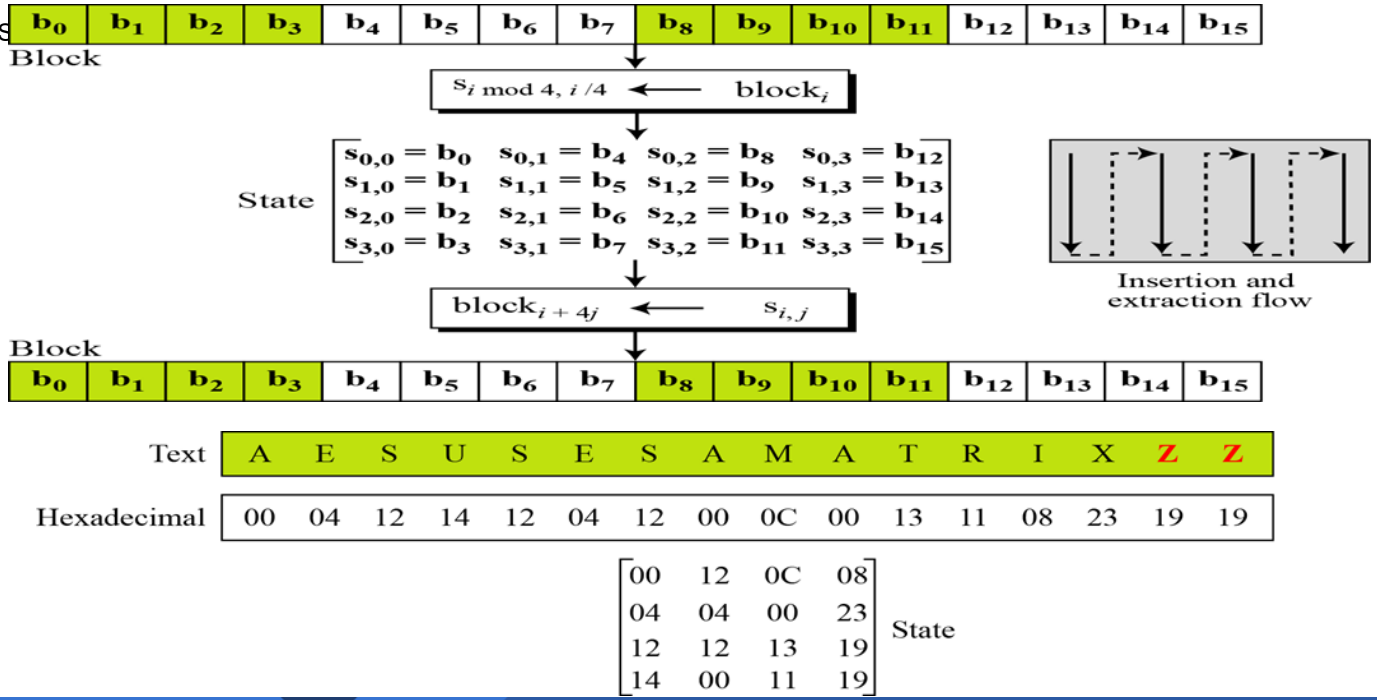
- designed by Rijmen-Daemen in Belgium
- has 128/192/256 bit keys, 128 bit data
- an **iterative** rather than **feistel** cipher
  - processes data as block of 4 columns of 4 bytes
  - operates on entire data block in every round
- designed to be:
  - resistant against known cryptanalysis attacks
  - speed and code compactness on many CPUs
  - design simplicity

- AES is a **non-Feistel** cipher that encrypts and decrypts a data block of 128 bits arranged in a matrix of 4 columns of 4 bytes named **state**.
- It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds. Key is **expanded** to array of words (state).
- In each round, the state undergoes:
  1. **Byte substitution** (1 S-box used on every byte)
  2. **Shift rows** (permute bytes between groups/columns)
  3. **Mix columns** (subs using matrix multiply of groups)
  4. **Add round key** (XOR state with key material)

AES Structure



AES S

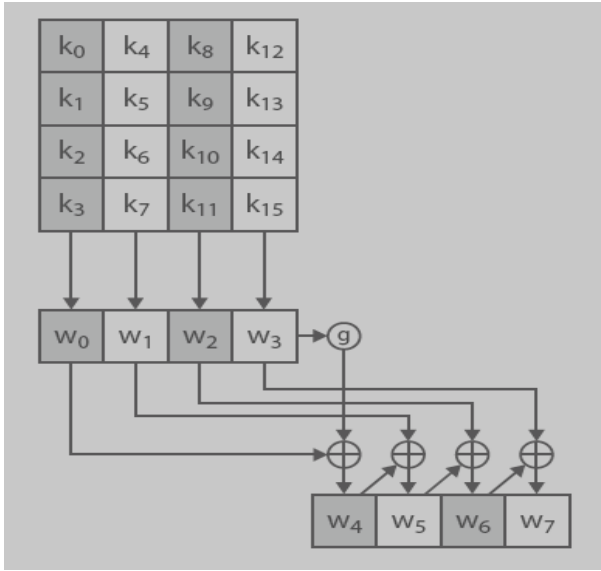


AES Structure- Key Expansion

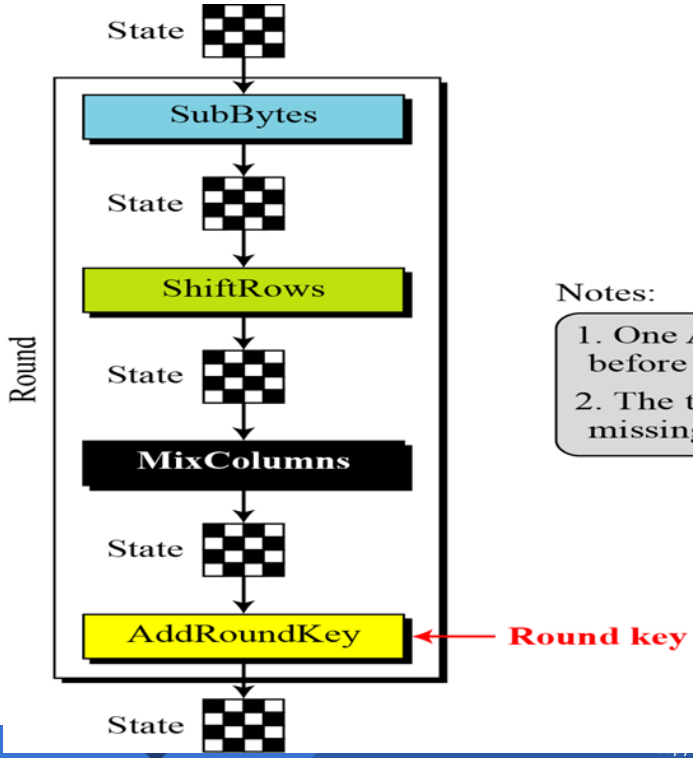
- **Objective**: To create round keys for each round, AES uses a key-expansion process.
- If the number of rounds is N_r , the key-expansion routine creates N_{r+1} 128-bit round keys from one single 128-bit cipher key.
- takes 128-bit (16-byte) key and expands into array of 44/52/60 32-bit words

AES Structure- Key Expansion

- start by copying key into first 4 words
- then loop creating words that depend on values in previous & 4 back words
  - in 3 of 4 cases just XOR these together
  - 1st word in 4 has rotate + S-box + XOR round constant on previous, before XOR 4th back



AES Structure- Round

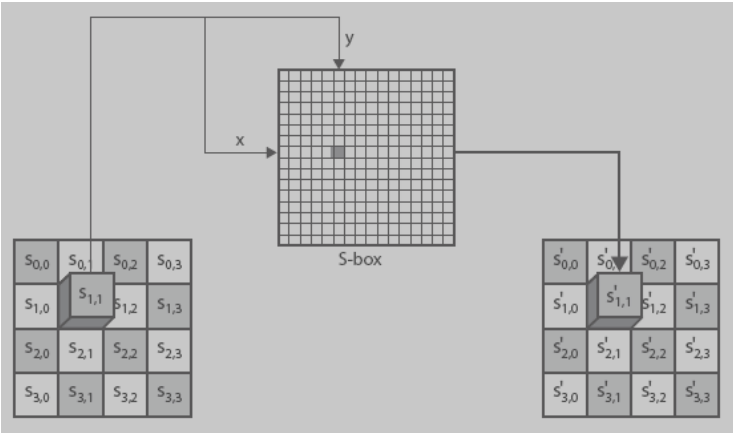


Notes:

1. One AddRoundKey is applied before the first round.
2. The third transformation is missing in the last round.

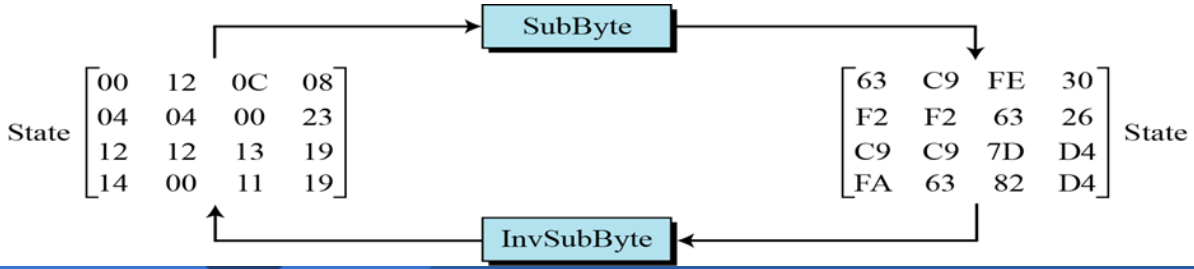
AES Structure- *SubBytes*

- **Byte Substitution (SubBytes)**
  - It is used to substitute a byte, we interpret the byte as two hexadecimal digits.



- **Example**

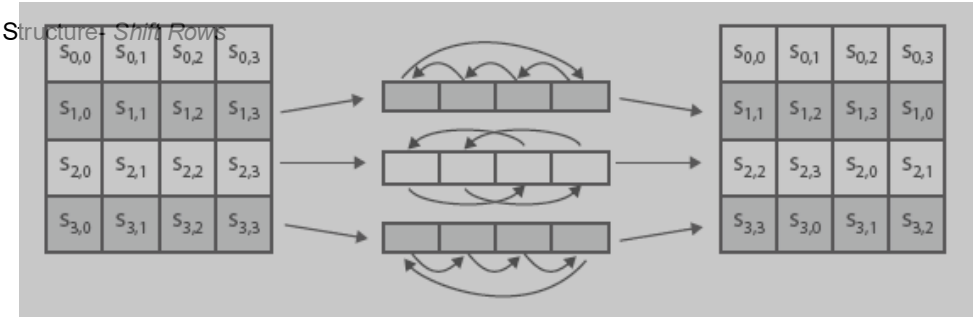
		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	a	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	b	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	c	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	d	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	e	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	f	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D



AES Structure- *Shift Rows*

- **Shift Rows**
  - a circular byte shift to left in each row
  - decrypt inverts using shifts to right
  - since state is processed by columns, this step permutes bytes between the columns

AES Structure- *Shift Rows*

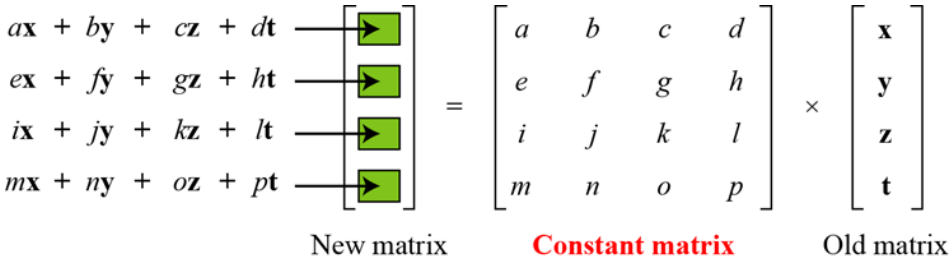


87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

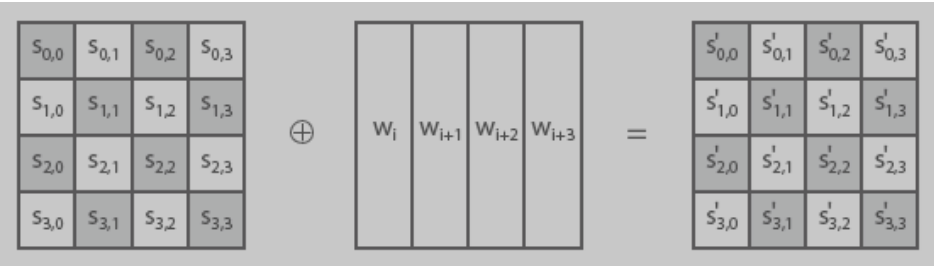
- **Mix Columns**
  - We mix bytes using matrix multiplication
  - each column is processed separately
  - each byte is replaced by a value dependent on all 4 bytes in the column



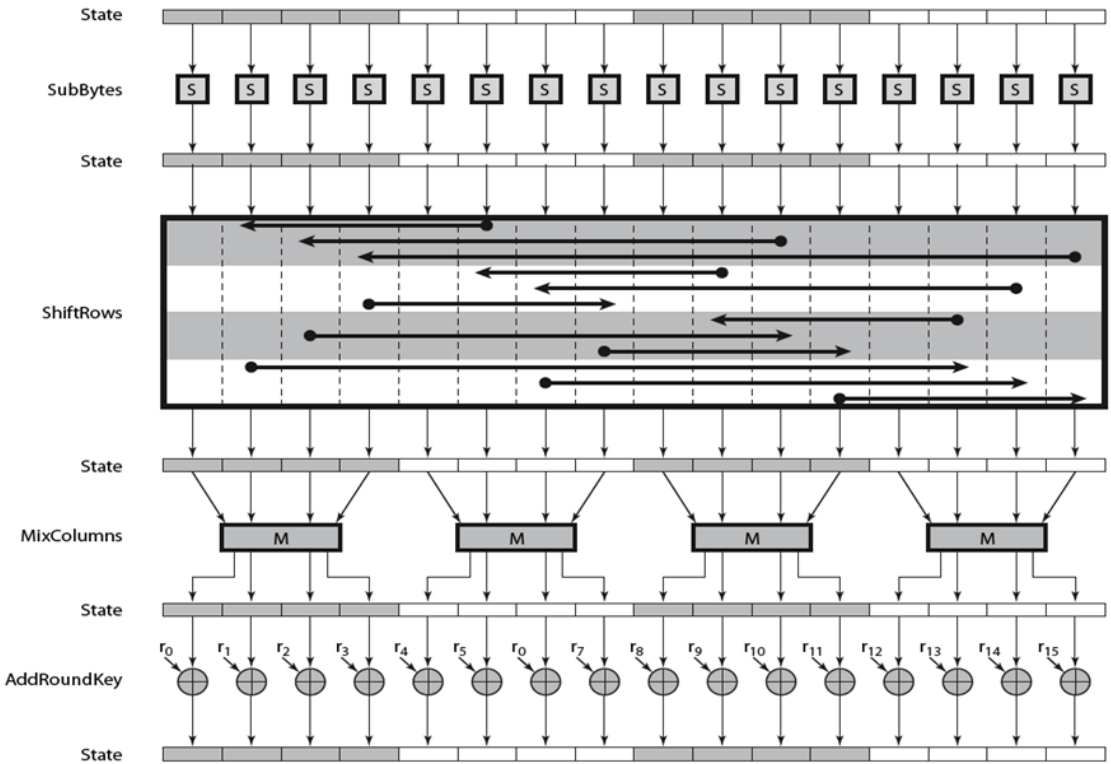
AES Structure- *Add Round Key*

- Add Round Key
  - XOR state with 128-bits of the round key
  - again processed by column (though effectively a series of byte operations)
  - inverse for decryption identical
  - since XOR own inverse, with reversed keys
  - designed to be as simple as possible
  - a form of Vernam cipher on expanded key
  - requires other stages for complexity / security

AES Structure- *Add Round Key*



AES Encryption Round



AES Summary

- has a simple structure
- only AddRoundKey uses key
- AddRoundKey a form of Vernam cipher
- each stage is easily reversible
- decryption uses keys in reverse order
- decryption does recover plaintext
- final round has only 3 stages
- **Review**:

www.securityfit.cz/download/kib/**rijndael_ingles2004.swf**

Module Summary

- This module has discussed cryptographic techniques, different encryption algorithms, and hashing algorithms
- It has discussed different cryptography tools and hash calculators