Skim read the info on the link below (Link is in the chat).

UK Home Office open letter to Mark Zuckerberg about end-

to-end encryption.

https://homeofficemedia.blog.gov.uk/2019/11/05/factsheet-encryption/

Symmetric Encryption

Overview

- Key bits – Symmetric not a history
- Computationally secure cipher
- Feistel Structure
- DES
- 3DES
- AES
- End-to-end encryption

Classified along three independent dimensions:

The type of operations used for transforming plaintext to ciphertext

- Substitution – each element in the plaintext is mapped into another element
- Transposition – elements in plaintext are rearranged

The way in which the plaintext is processed

- Block cipher – processes input one block of elements at a time
- Stream cipher – processes the input elements continuously

The number of keys used

- Sender and receiver use same key – symmetric
- Sender and receiver each use a different key - asymmetric

Completed last week | Completed on Tuesday | From Today

Symmetric Encryption

- Also referred to as:
  - Conventional encryption
  - Secret-key or single-key encryption
- Only alternative before public-key encryption in 1970's
  - Still most widely used alternative
- Has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret key
  - Ciphertext
  - Decryption algorithm

Computationally Secure Encryption Schemes

- Encryption is computationally secure if:
  - Cost of breaking cipher exceeds value of information
  - Time required to break cipher exceeds the useful lifetime of the information
- Usually very difficult to estimate the amount of effort required to break
- Can estimate time/cost of a brute-force attack -

  did this in last lecture [timing consideration]

- Used in block ciphers
- No of steps

1) Plaintext divided into Left and Right
2) Function is used on the right text and also receive key (function depends on what algorithm you use e.g. DES or 3DES)
3) Results of function is XOR with plaintext from left
4) Plaintext of right goes to left
5) Results of XOR goes to right
6) These new left and right texts become inputs for further rounds

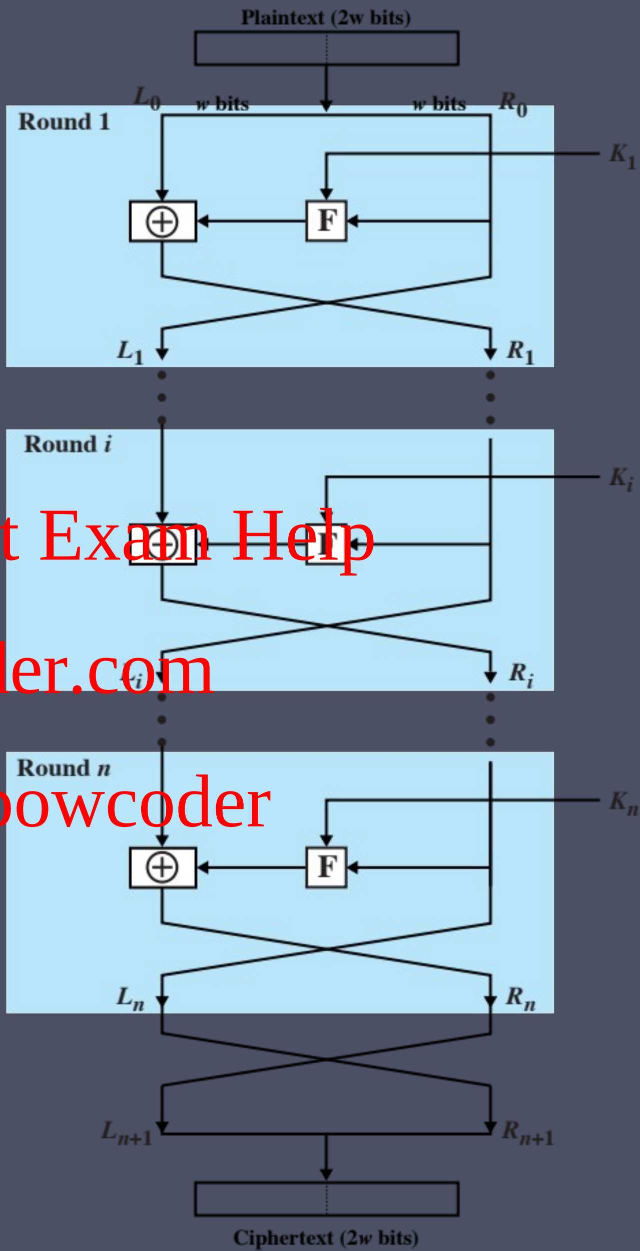
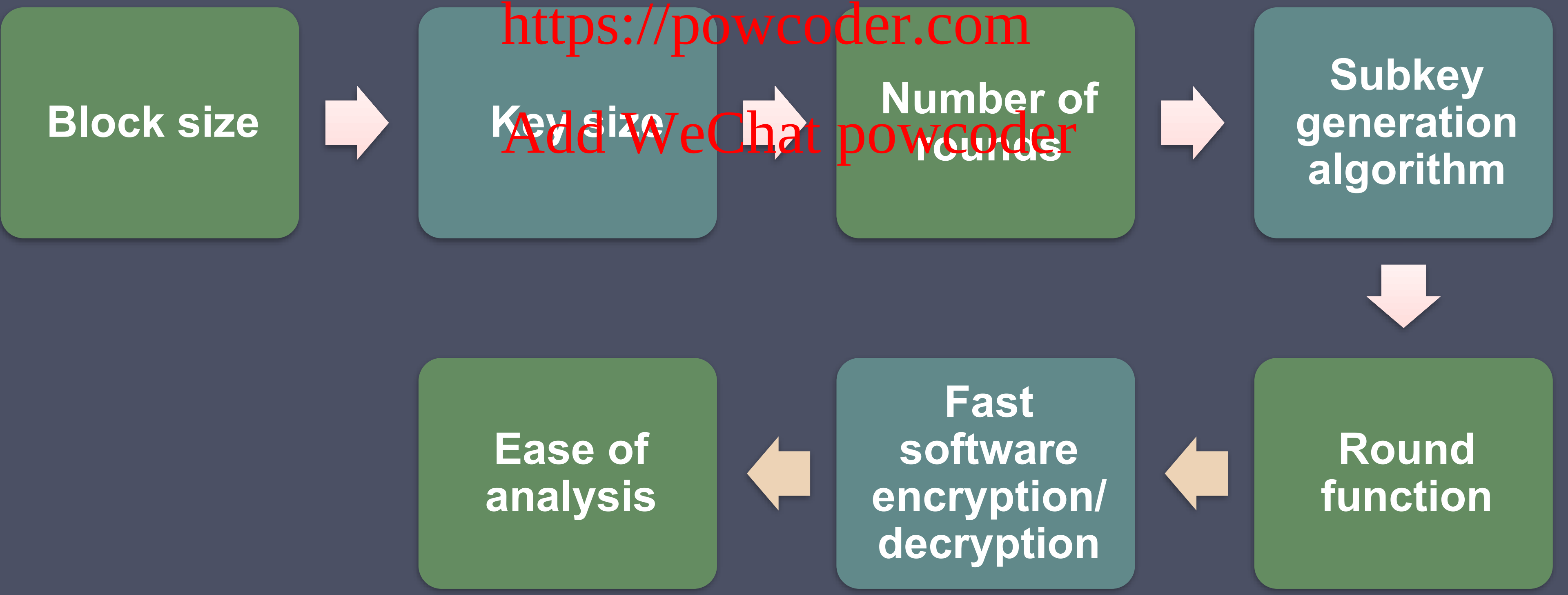


Figure 20.1 Classical Feistel Network

Block Cipher Structure

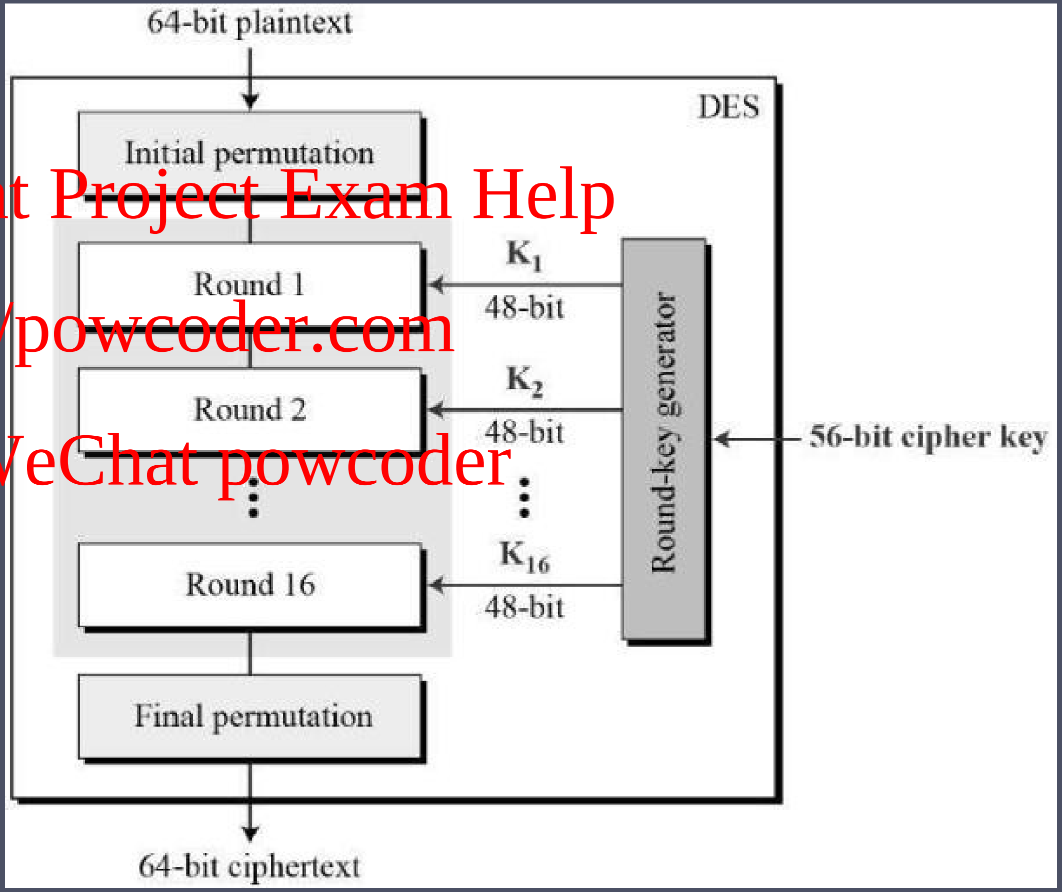
- Symmetric block cipher consists of:
  - A sequence of rounds
  - With substitutions and permutations controlled by key
- Parameters and design features:



- Most widely used encryption scheme
- Adopted in 1977 by National Bureau of Standards (Now NIST)
- FIPS PUB 46
- Algorithm is referred to as the Data Encryption Algorithm (DEA)
- Minor variation of the Feistel network
- Used 16 rounds of Feistel cipher
- Block size 64 bits
- Key size is 64 bits but effective key size is 56 bits, 8 bits of the key are check bits (64 bits – 8 check bits = 56 bits key size)

Data Encryption Standard (DES)

- Key processes in DES:
  1) Permutation
  2) Round function
  3) Key generation



DES process

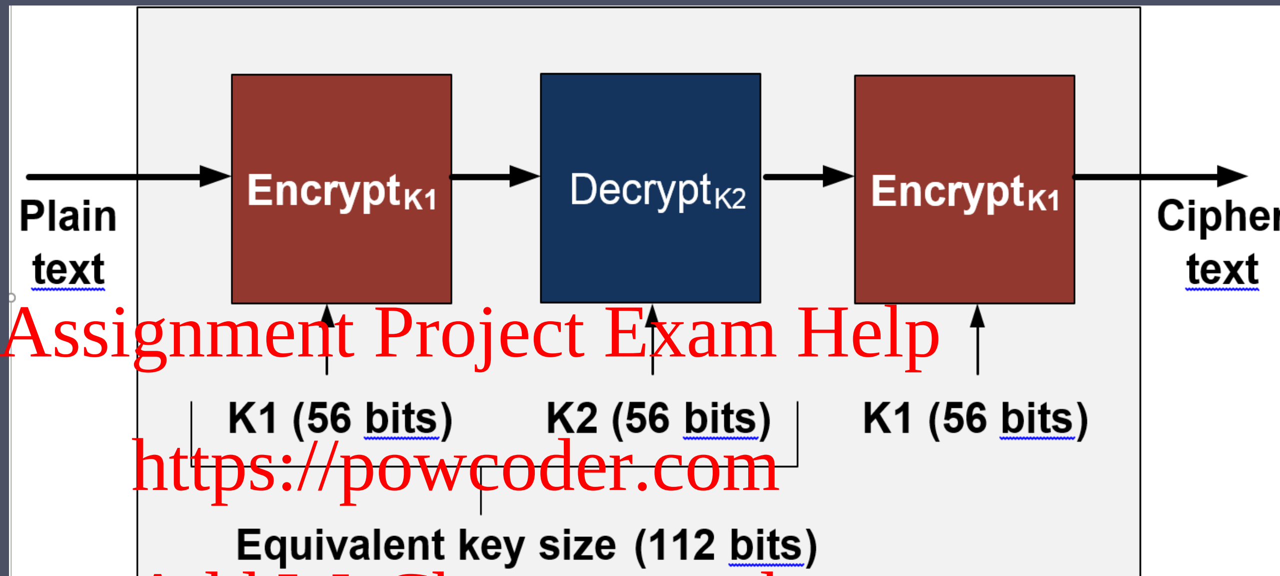
1	2	3	4	5	6	7	8
9	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	64

- Plaintext is represented in 64 bits
- Permutation in DES

In initial permutation 58 bit becomes first position and 7 becomes last

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

3DES

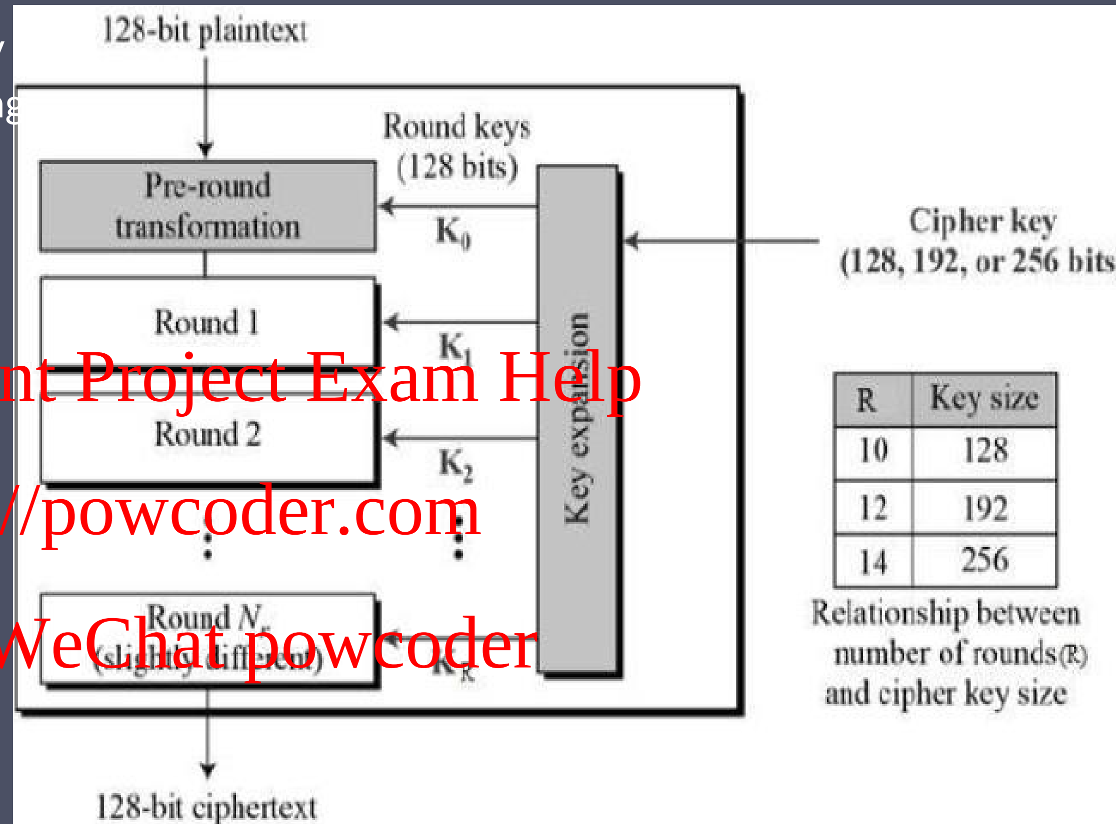


- A quick solution to overcome the DES weakness was 3-DES
- To save time and money
- K3==K1 2 keys of 56 bits 112 bits
- Problem: too slow

AES

- DES→ Key size too small, exhaustive key search possible with increasing computing power
- 3-DES→ too slow
- Alternative is AES
- Key features of AES:

1) Secret or symmetric cipher
2) Block cipher
3) 128-bit data, 128/192/256-bit keys
4) Stronger and faster than Triple-DES
5) Not based on Feistel structure
6) Iterative - a no of substitution & permutation
7) Performed operations on bytes rather than on bits
8) 128 bits – 16 bytes: arranged in 4 x 4 matrix
9) No of rounds depend on key size; 10 for 128 bits, 12 192 bits and 14 for 256 bits
10) Each round use a unique key



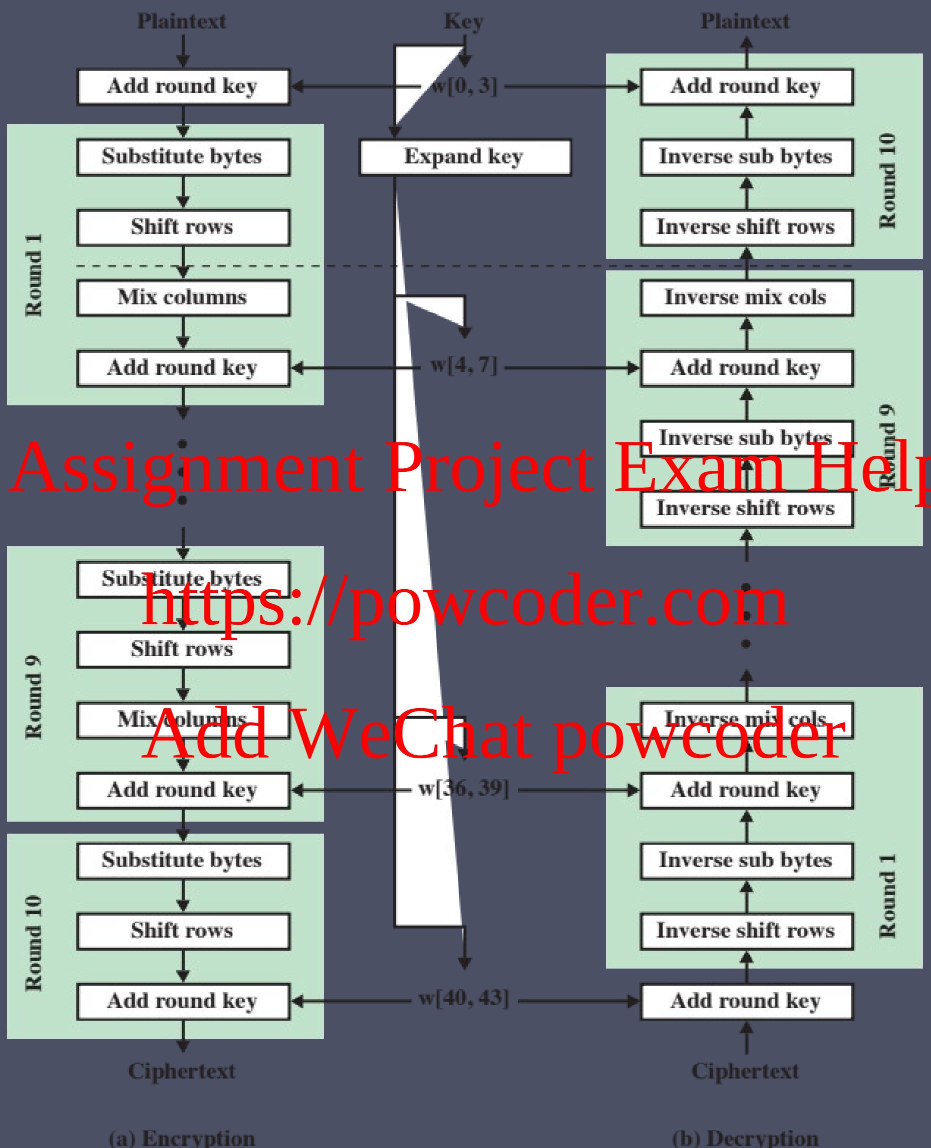


Figure 20.3 AES Encryption and Decryption

Plaintext -- Welcome To Computer

16 bytes = 128 bits AES block,
1byte for each character

Text	W	E	L	C	O	M	T	O	C	O	M	P	U	T	E	R

Suppose this is Hex 57 65 6c 63 6f 6d 65 54 6f 43 6f 6d 70 75 74 65

Don’t forget about padding

State

57	6f		
65	--	--	--
6c	--	--	--
63	--	--	--

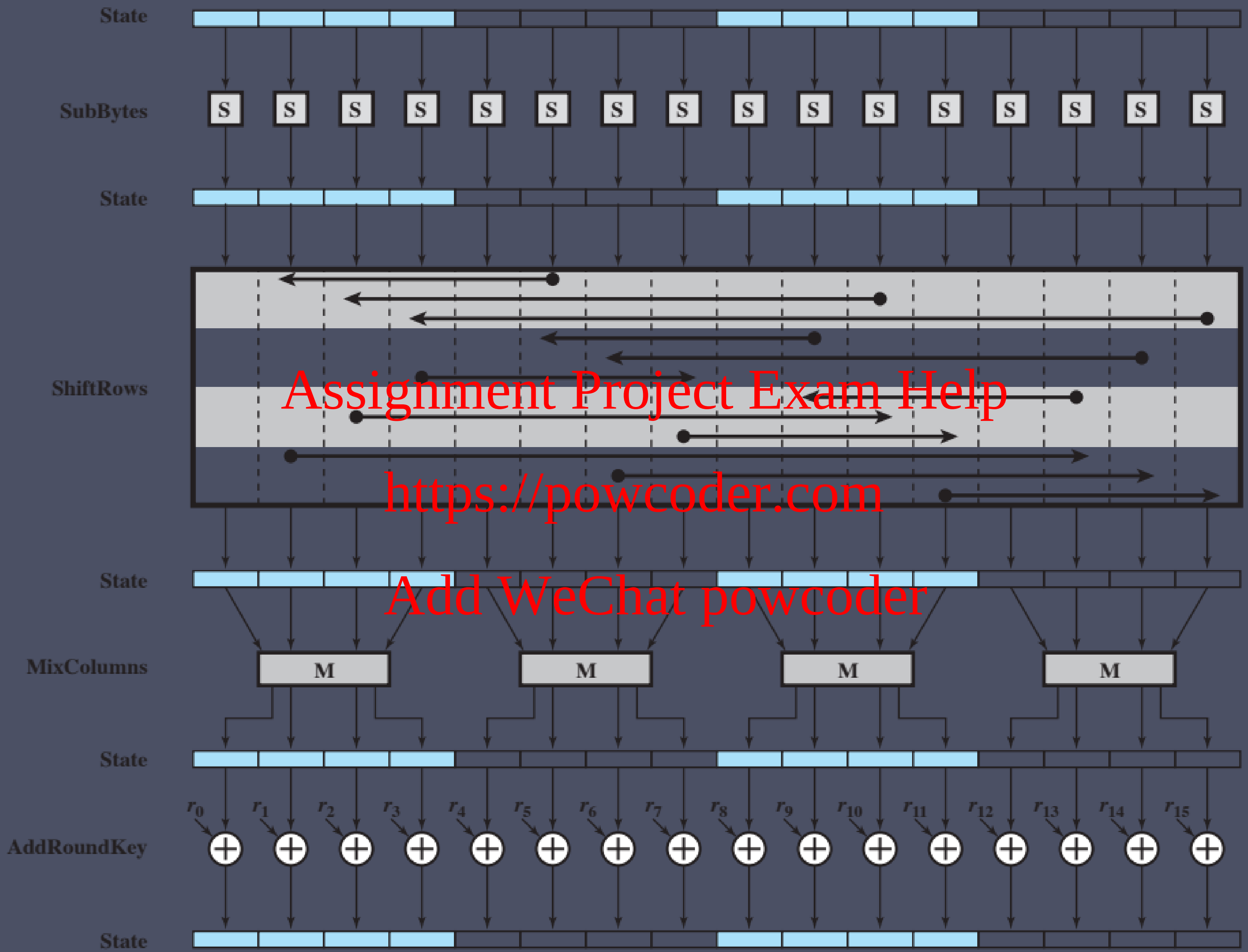


Figure 20.4 AES Encryption Round

Table 20.2 AES S-Boxes

(a) S-box

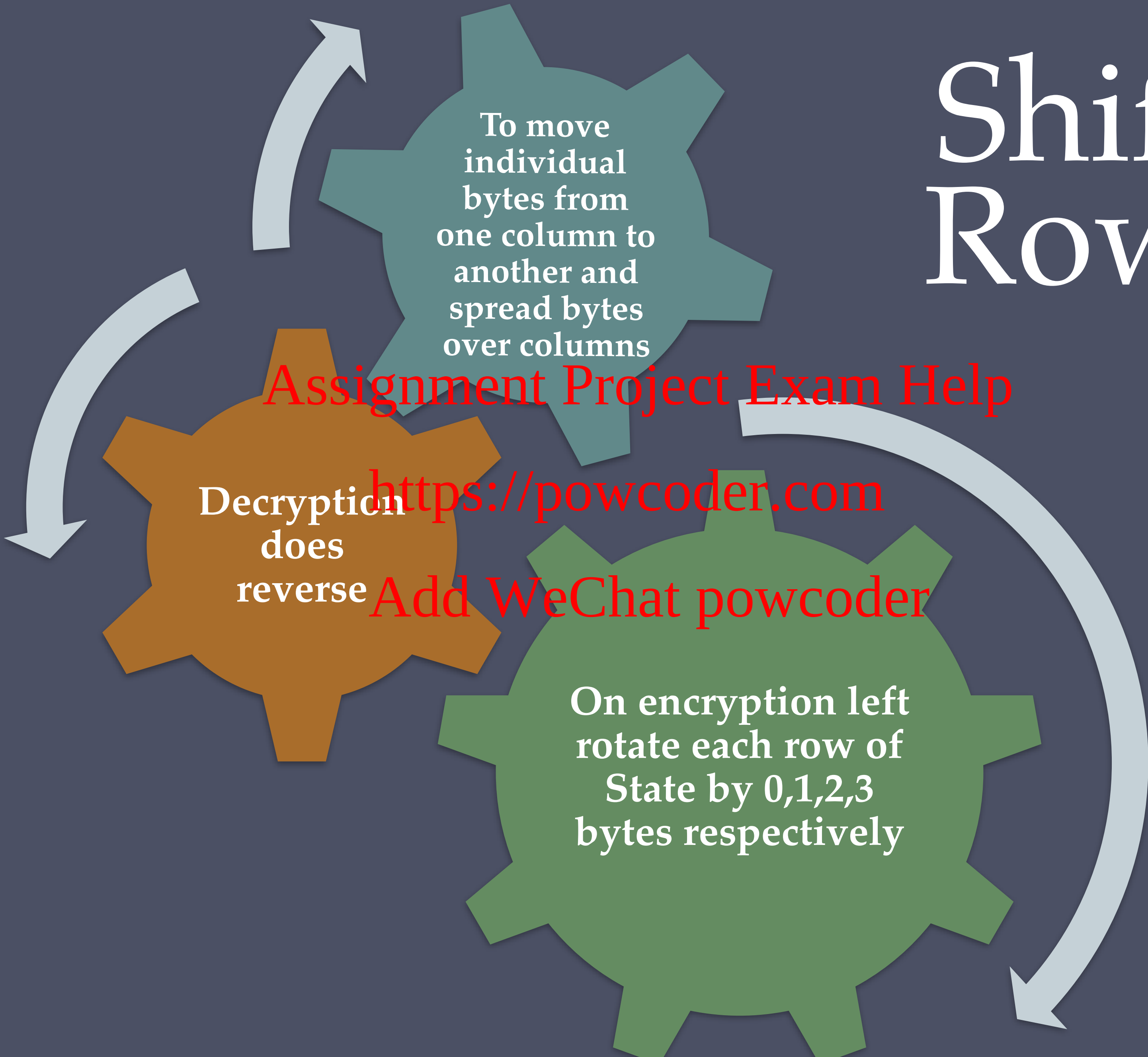
		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3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

Table 20.2 AES S-Boxes

(b) Inverse S-box

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
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

Shift Rows


To move individual bytes from one column to another and spread bytes over columns
Decryption does reverse
On encryption left rotate each row of State by 0,1,2,3 bytes respectively

Mix Columns and Add Key

- Mix columns
  - Operates on each column individually
  - Mapping each byte to a new value that is a function of all four bytes in the column

$$\begin{bmatrix} SX & 0 & 0 & 0 \\ 0 & SY & 0 & 0 \\ 0 & 0 & SZ & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix} = \begin{pmatrix} SX \cdot x \\ SY \cdot y \\ SZ \cdot z \\ 1 \end{pmatrix}$$

  - Use of equations over finite fields

A finite field or Galois field is a field that contains a finite number of elements. As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction and division are defined and satisfy certain basic rules

  - To provide good mixing of bytes in column
- Add round key
  - Simply XOR State with bits of expanded key
  - Security from complexity of round key expansion and other stages of AES

Key Distribution

- The means of delivering a key to two parties that wish to exchange data without allowing others to see the key
- Two parties (A and B) can achieve this by:

1. A key could be selected by A and physically delivered to B
2. A third party could select the key and physically deliver it to A and B
3. If A and B have previously and recently used a key, one party could transmit the new key to the other, encrypted using the old key
4. If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B

1. Host sends packet requesting connection.
2. Security service buffers packet; asks KDC for session key.
3. KDC distributes session key to both hosts.
4. Buffered packet transmitted.

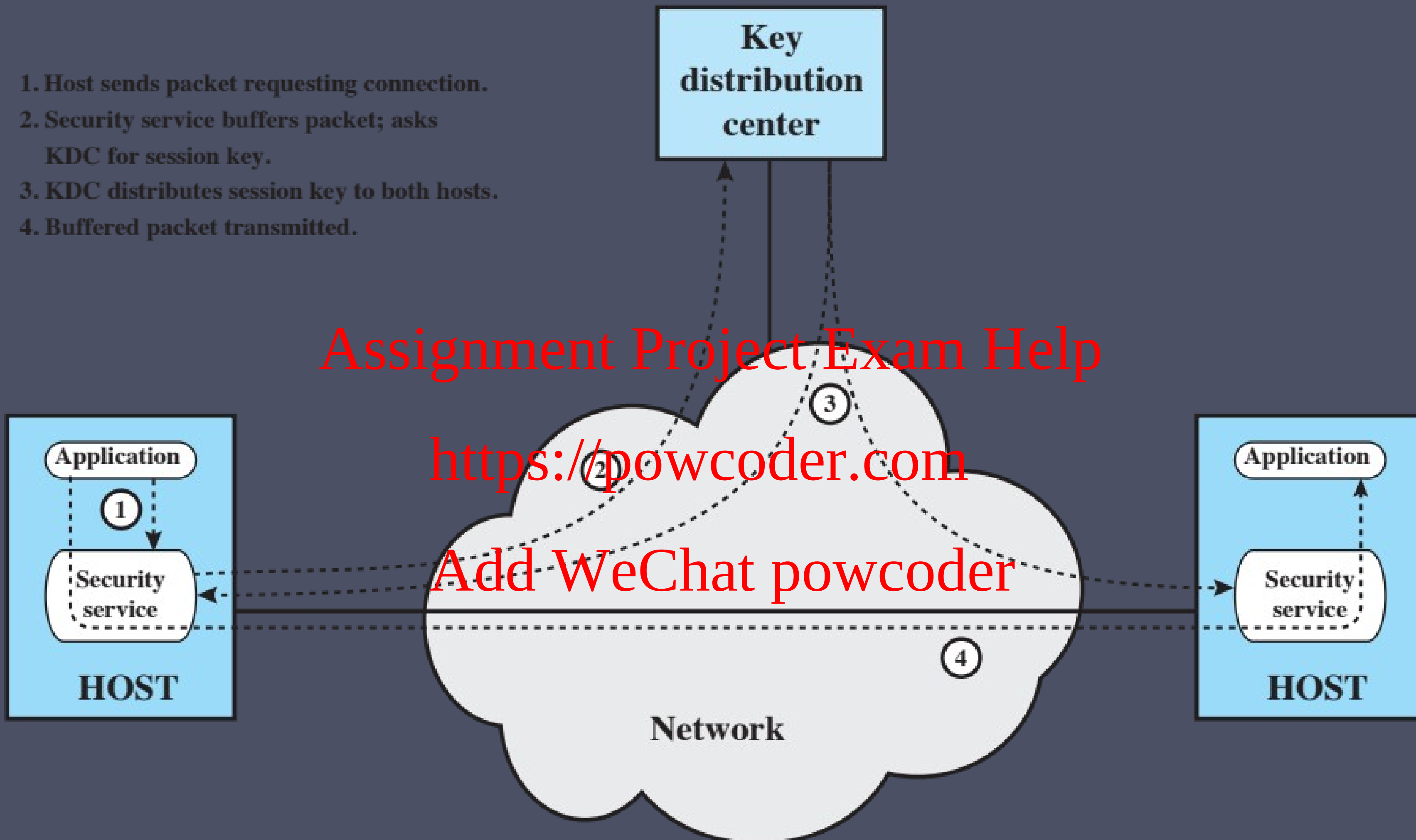


Figure 20.10 Automatic Key Distribution for Connection-Oriented Protocol

Criminals use of end-to-end encryption

-

- https://privacyinternational.org/news-analysis/3242/no-uk-hasnt-just-signed-treaty-meaning-end-end-end-encryption