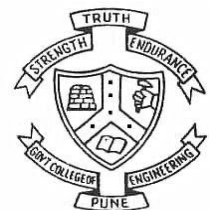


Cryptology and Network Security

Unit-III

Session 18

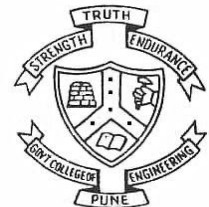
Dr. V. K. Pachghare



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

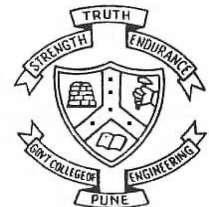
International Data Encryption Algorithm

(IDEA)



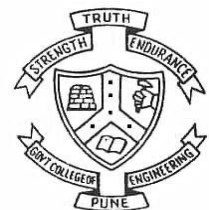
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Simplified IDEA Example

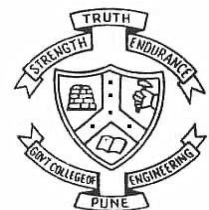


Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

- Plaintext block -16-bit
- Key - 32-bit
- Rounds: four identical rounds and a “half round”
- So, $4 \times 6 + 4 = 28$ subkeys



KEY: 11011100011011110011111101011001



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

KEY: 11011100011011110011111101011001

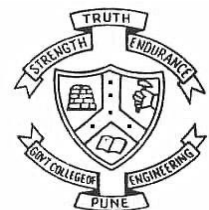
Divide the key into 8 nibbles (groups). (Each group having 4 bits)



KEY: 11011100011011110011111101011001

Divide the key into 8 nibbles (groups). (Each group having 4 bits)

1101 1100 0110 1111 0011 1111 0101 1001

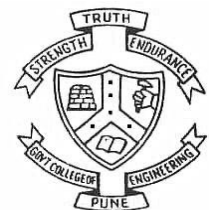


KEY: 11011100011011110011111101011001

Divide the key into 8 nibbles (groups). (Each group having 4 bits)

1101 1100 0110 1111 0011 1111 0101 1001

- The first six nibbles are used as the subkeys for round 1

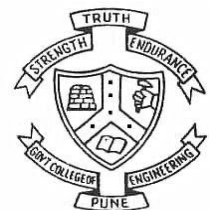


KEY: 11011100011011110011111101011001

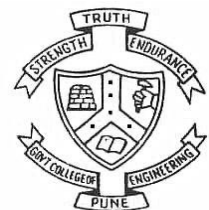
Divide the key into 8 nibbles (groups). (Each group having 4 bits)

1101 1100 0110 1111 0011 1111 **0101 1001**

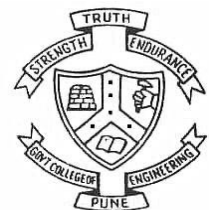
- The first six nibbles are used as the subkeys for round 1
- The remaining two nibbles are the first two subkeys for round 2



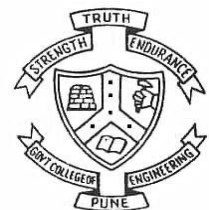
- Then the bits are shifted cyclically 6 places to the left



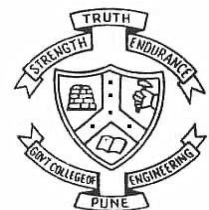
- Then the bits are shifted cyclically 6 places to the left
- The new 32-bit string is split into eight nibbles that become the next eight subkeys
-



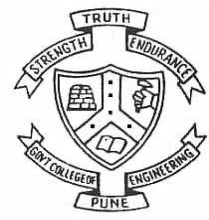
- Then the bits are shifted cyclically 6 places to the left
- The new 32-bit string is split into eight nibbles that become the next eight subkeys
- The first four of these nibbles are used to complete the subkeys needed for round 2, and



- Then the bits are shifted cyclically 6 places to the left
- The new 32-bit string is split into eight nibbles that become the next eight subkeys
- The first four of these nibbles are used to complete the subkeys needed for round 2, and
- The remaining four subkeys are used in round 3.



- Then the bits are shifted cyclically 6 places to the left
- The new 32-bit string is split into eight nibbles that become the next eight subkeys
- The first four of these nibbles are used to complete the subkeys needed for round 2, and
- The remaining four subkeys are used in round 3.
- The shifting and splitting process is repeated until all 28 subkeys are generated



Message:-1111101111011010

Key:- 101010011101111101100101111000011

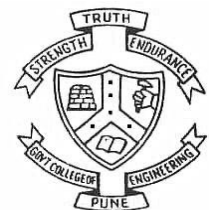


Split the message as a group of 4 bit each

P_1 , P_2 , P_3 and P_4 are plaintext blocks

Message:-1111 1011 1101 1010

Key:- 1010 1001 1101 1111 0110 0101 1100 0011

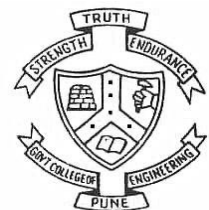


Key Generation

	Round -1	Round - 2	Round - 3	Round - 4	Round -5
Key -1	1010	1100	0111	0101	1001
Key - 2	1001	0011 *	0000	1100	0111
Key - 3	1101	0111	1110	0011	0000
Key - 4	1111	0111	1010 *	1010	1110
Key - 5	0110	1101	1111	1001	
Key - 6	0101	1001	0110	1101*	



- $P_1: 1111$
- $P_2: 1011$
- $P_3: 1101$
- $P_4: 1010$

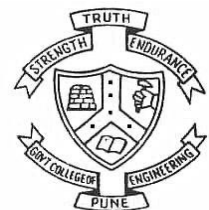


Round – 1

$$S1 = P1 \cdot K1$$

$$\begin{array}{r} 1 \ 1 \ 1 \ 1 \ (15) \\ \otimes \ 1 \ 0 \ 1 \ 0 \ (10) \\ \hline 1 \ 1 \ 1 \ 0 \ (14) \end{array}$$

$$15 \times 14 \bmod (2^4 + 1) = 14$$



Round – 1

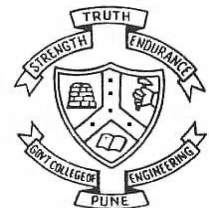
$$S1 = P1 \cdot K1$$

$$S2 = P2 + K2$$

$$\otimes \begin{array}{rrrr} 1 & 1 & 1 & 1 (15) \\ 1 & 0 & 1 & 0 (10) \\ \hline 1 & 1 & 1 & 0 (14) \end{array}$$

$$\begin{array}{rrrr} 1 & 0 & 1 & 1 (11) \\ 1 & 0 & 0 & 1 (9) \\ \hline 0 & 1 & 0 & 0 (4) \end{array}$$

$$(11+9) \bmod 16 = 4$$



Round – 1

$$S1 = P1 \cdot K1$$

$$\begin{array}{cccc} 1 & 1 & 1 & 1 \end{array} (15)$$

$$\otimes \begin{array}{cccc} 1 & 0 & 1 & 0 \end{array} (10) \\ \hline \begin{array}{cccc} 1 & 1 & 1 & 0 \end{array} (14)$$

$$15 \times 14 \bmod 17 = 14$$

$$S2 = P2 + K2$$

$$\begin{array}{cccc} 1 & 0 & 1 & 1 \end{array} (11)$$

$$\begin{array}{cccc} 1 & 0 & 0 & 1 \end{array} (9) \\ \hline \begin{array}{cccc} 0 & 1 & 0 & 0 \end{array} (4)$$

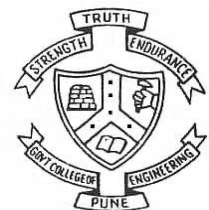
$$(11 + 9) \bmod 16 = 4$$

$$S3 = P3 + K3$$

$$\begin{array}{cccc} 1 & 1 & 0 & 1 \end{array} (13)$$

$$\begin{array}{cccc} 1 & 1 & 0 & 1 \end{array} (13) \\ \hline \begin{array}{cccc} 1 & 0 & 1 & 0 \end{array} (10)$$

$$(13 + 13) \bmod 16 = 10$$



Round – 1

	$S1 = P1 \cdot K1$	$S2 = P2 + K2$	$S3 = P3 + K3$	$S4 = P4 \cdot K4$
	1 1 1 1 (15)	1 0 1 1 (11)	1 1 0 1	1 0 1 0
\otimes	$\frac{1 0 1 0 (10)}{1 1 1 0 (14)}$	$\frac{1 0 0 1 (9)}{0 1 0 0 (4)}$	$\frac{1 1 0 1}{1 0 1 0}$	$\frac{1 1 1 1}{1 1 1 0}$
	$15 \times 14 \bmod 17 = 14$	$(11 + 9) \bmod 16 = 4$		

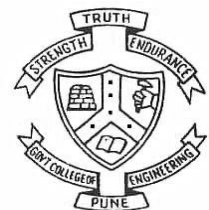


Round – 1

$$\begin{array}{l}
 \text{S1} = \text{P1} \cdot \text{K1} \quad \text{S2} = \text{P2} + \text{K2} \quad \text{S3} = \text{P3} + \text{K3} \quad \text{S4} = \text{P4} \cdot \text{K4} \\
 \begin{array}{cccc}
 1 & 1 & 1 & 1 \text{ (15)} \\
 1 & 0 & 1 & 0 \text{ (10)} \\
 \hline
 1 & 1 & 1 & 0 \text{ (14)}
 \end{array}
 \quad
 \begin{array}{cccc}
 1 & 0 & 1 & 1 \text{ (11)} \\
 1 & 0 & 0 & 1 \text{ (9)} \\
 \hline
 0 & 1 & 0 & 0 \text{ (4)}
 \end{array}
 \quad
 \begin{array}{cccc}
 1 & 1 & 0 & 1 \\
 1 & 1 & 0 & 1 \\
 \hline
 1 & 0 & 1 & 0
 \end{array}
 \quad
 \begin{array}{cccc}
 1 & 0 & 1 & 0 \\
 1 & 1 & 1 & 1 \\
 \hline
 1 & 1 & 1 & 0
 \end{array} \\
 15 \times 14 \bmod 17 = 14 \quad (11+9) \bmod 16 = 4
 \end{array}$$

$$\text{S5} = \text{S1} \text{ xor } \text{S3}$$

$$\begin{array}{cccc}
 1 & 1 & 1 & 0 \\
 1 & 0 & 1 & 0 \\
 \hline
 0 & 1 & 0 & 0
 \end{array}$$



Round – 1

$$S1 = P1 \cdot K1$$

$$\begin{array}{r} 1 \ 1 \ 1 \ 1 \ (15) \\ \otimes \ 1 \ 0 \ 1 \ 0 \ (10) \\ \hline 1 \ 1 \ 1 \ 0 \ (14) \end{array}$$

$$15 \times 14 \bmod 17 = 14$$

$$S2 = P2 + K2$$

$$\begin{array}{r} 1 \ 0 \ 1 \ 1 \ (11) \\ 1 \ 0 \ 0 \ 1 \ (9) \\ \hline 0 \ 1 \ 0 \ 0 \ (4) \end{array}$$

$$(11 + 9) \bmod 16 = 4$$

$$S3 = P3 + K3$$

$$\begin{array}{r} 1 \ 1 \ 0 \ 1 \\ 1 \ 1 \ 0 \ 1 \\ \hline 1 \ 0 \ 1 \ 0 \end{array}$$

$$S4 = P4 \cdot K4$$

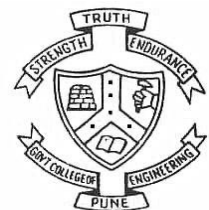
$$\begin{array}{r} 1 \ 0 \ 1 \ 0 \\ 1 \ 1 \ 1 \ 1 \\ \hline 1 \ 1 \ 1 \ 0 \end{array}$$

$$S5 = S1 \text{ xor } S3$$

$$\begin{array}{r} 1 \ 1 \ 1 \ 0 \\ 1 \ 0 \ 1 \ 0 \\ \hline 0 \ 1 \ 0 \ 0 \end{array}$$

$$S6 = S2 \text{ xor } S4$$

$$\begin{array}{r} 0 \ 1 \ 0 \ 0 \\ 1 \ 1 \ 1 \ 0 \\ \hline 1 \ 0 \ 1 \ 0 \end{array}$$



$$S7 = S5 \cdot K5$$

$$\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 1 & 1 & 1 \end{array}$$

$$S10 = S7 + S9$$

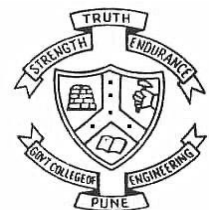
$$\begin{array}{cccc} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 0 & 0 \end{array}$$

$$S8 = S6 + S7$$

$$\begin{array}{cccc} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 \end{array}$$

$$S9 = S8 \cdot K6$$

$$\begin{array}{cccc} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 \end{array}$$



$$S11 = S9 \text{ xor } S1 \quad S12 = S10 \text{ xor } S2$$

$$S13 = S9 \text{ xor } S3 \quad S14 = S10 \text{ xor } S4$$

$$\begin{array}{cccc} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & 1 \end{array}$$

$$\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 \end{array}$$

$$\begin{array}{cccc} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 1 \end{array}$$

$$\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ \hline 0 & 0 & 1 & 0 \end{array}$$

$$P1 = S11$$

$$P2 = S12$$

$$P3 = S13$$

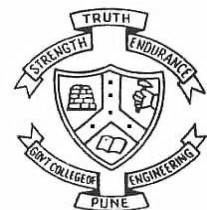
$$P4 = S14$$

$$1 \quad 0 \quad 1 \quad 1$$

$$1 \quad 0 \quad 0 \quad 0$$

$$1 \quad 1 \quad 1 \quad 1$$

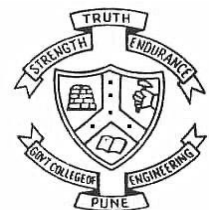
$$0 \quad 0 \quad 1 \quad 0$$



Generate the key for decryption

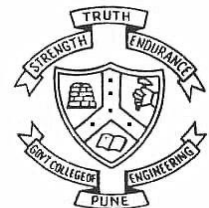
- **Key:**

10101001110111110110010111000011



Addition Mod 16

- Suppose the number is n
- $n \bmod 16 = (n + m) \bmod 16 = 0$



Addition Mod 16

- Suppose the number is n
- $n \bmod 16 = (n + m) \bmod 16 = 0$
- Where m is the addition modulo 16 of n .
- i.e. $m = 16 - n$



Addition Mod 16

- Suppose the number is n
- $n \bmod 16 = (n + m) \bmod 16 = 0$
- Where m is the addition modulo 16 of n .
- i.e. $m = 16 - n$
- Suppose $n = 1$ then $m = 16 - 1 = 15$
- $n = 2$ then $m = 16 - 2 = 14$



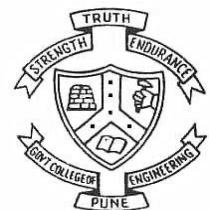
Addition Mod 16

- Suppose the number is n
- $n \bmod 16 = (n + m) \bmod 16 = 0$
- Where m is the addition modulo 16 of n .
- i.e. $m = 16 - n$
- Suppose $n = 1$ then $m = 16 - 1 = 15$
- $n = 2$ then $m = 16 - 2 = 14$
- **Note: If $n = 0$ then $m = 0$**



Inverse of nibbles for addition modulo 16

Number in binary	Number in decimal	Inverse in binary	Inverse in decimal
0000	0	0000	0
0001	1	1111	15
0010	2	1110	14
0011	3	1101	13
0100	4	1100	12
0101	5	1011	11
0110	6	1010	10
0111	7	1001	9
1000	8	1000	8
1001	9	0111	7
1010	10	0110	6
1011	11	0101	5
1100	12	0100	4
1101	13	0011	3
1110	14	0010	2
1111	15	0001	1



Multiplication Mod 17

- Suppose the number is n , Therefore $n * m \bmod 17 = 1$
- m is the multiplicative inverse of $n \bmod 17$.



Multiplication Mod 17

- Suppose the number is n , Therefore $n * m \bmod 17 = 1$
- m is the multiplicative inverse of $n \bmod 17$.
- For $n=1$
- $1 * m \bmod 17 = 1 = m$



Multiplication Mod 17

- Suppose the number is n , Therefore $n * m \bmod 17 = 1$
- m is the multiplicative inverse of $n \bmod 17$.
- For $n = 1$
- $1 * m \bmod 17 = 1 = m$
- For $n = 2$, $m = 9$
- $2 * 9 \bmod 17 = 18 \bmod 17 = 1$
- So 9 and 2 are the multiplicative inverse of each other



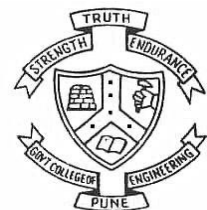
Multiplication Mod 17

- Suppose the number is n , Therefore $n * m \bmod 17 = 1$
- m is the multiplicative inverse of $n \bmod 17$.
- For $n = 1$
- $1 * m \bmod 17 = 1 = m$
- For $n = 2$, $m = 9$
- $2 * 9 \bmod 17 = 18 \bmod 17 = 1$
- So 9 and 2 are the multiplicative inverse of each other
- **Note: If $n = 0$ then consider $n = 16$ and $m = 16$**



Inverses of nibbles for multiplication modulo 17

Number in binary	Number in decimal	Inverse in binary	Inverse in decimal
0001	1	0001	1
0010	2	1001	9
0011	3	0110	6
0100	4	1101	13
0101	5	0111	7
0110	6	0011	3
0111	7	0101	5
1000	8	1111	15
1001	9	0010	2
1010	10	1100	12
1011	11	1110	14
1100	12	1010	10
1101	13	0100	4
1110	14	1011	11
1111	15	1000	8
0000	16 = -1	0000	16 = -1

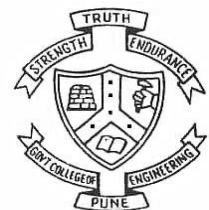


Key for encryption

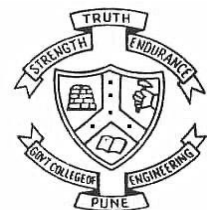
	Round -1	Round - 2	Round - 3	Round - 4	Round -5
Key -1	1010	1100	0111	0101	1001
Key - 2	1001	0011 *	0000	1100	0111
Key - 3	1101	0111	1110	0011	0000
Key - 4	1111	0111	1010 *	1010	1110
Key - 5	0110	1101	1111	1001	
Key - 6	0101	1001	0110	1101*	



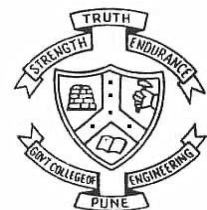
	(K_j^i)	Integer	Inverse in Integer	Z_j^i	Key for 1 st Round
(K_1^5)	1001	9	2 (Multiplicative modulo 17)	0010	Z_1^1



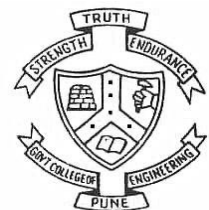
	(K_j^i)	Integer	Inverse in Integer	Z_j^i	Key for 1 st Round
(K_1^5)	1001	9	2 (Multiplicative modulo 17)	0010	Z_1^1
(K_2^5)	0111	7	9 (Addition modulo 16)	1001	Z_2^1



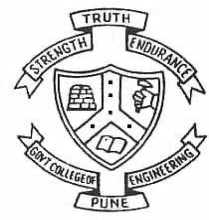
	(K_j^i)	Integer	Inverse in Integer	Z_j^i	Key for 1 st Round
(K_1^5)	1001	9	2 (Multiplicative modulo 17)	0010	Z_1^1
(K_2^5)	0111	7	9 (Addition modulo 16)	1001	Z_2^1
(K_3^5)	0000	0	0 (Addition modulo 16)	0000	Z_3^1



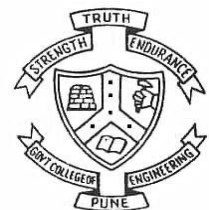
	(K_j^i)	Integer	Inverse in Integer	Z_j^i	Key for 1 st Round
(K_1^5)	1001	9	2 (Multiplicative modulo 17)	0010	Z_1^1
(K_2^5)	0111	7	9 (Addition modulo 16)	1001	Z_2^1
(K_3^5)	0000	0	0 (Addition modulo 16)	0000	Z_3^1
(K_4^5)	1110	14	11 (Multiplicative modulo 17)	1011	Z_4^1



	(K_j^i)	Integer	Inverse in Integer	Z_j^i	Key for 1 st Round
(K_1^5)	1001	9	2 (Multiplicative modulo 17)	0010	Z_1^1
(K_2^5)	0111	7	9 (Addition modulo 16)	1001	Z_2^1
(K_3^5)	0000	0	0 (Addition modulo 16)	0000	Z_3^1
(K_4^5)	1110	14	11 (Multiplicative modulo 17)	1011	Z_4^1
(K_5^4)	1001	9	9	1001	Z_5^1



	(K_j^i)	Integer	Inverse in Integer	Z_j^i	Key for 1 st Round
(K_1^5)	1001	9	2 (Multiplicative modulo 17)	0010	Z_1^1
(K_2^5)	0111	7	9 (Addition modulo 16)	1001	Z_2^1
(K_3^5)	0000	0	0 (Addition modulo 16)	0000	Z_3^1
(K_4^5)	1110	14	11 (Multiplicative modulo 17)	1011	Z_4^1
(K_5^4)	1001	9	9	1001	Z_5^1
(K_6^4)	1101	13	13	1101	Z_6^1

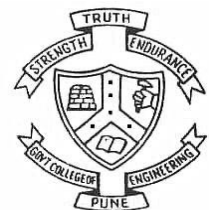


We can generate the keys as above for all 5 rounds

	Round -1	Round - 2	Round - 3	Round - 4	Round -5
Key -1	0010	0111	0101	1010	1100
Key - 2	1001	0100	0000	1101	0111
Key - 3	0000	1101	0010	1001	0011
Key - 4	1011	1100	1100	0101	1000
Key - 5	1001	1111	1101	0110	
Key - 6	1101	0110	1001	0101	



Questions ?



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education