

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_p(x)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Let also the key schedule be derived from a 32-bit key K in a cyclic manner by considering 16 consecutive bits beginning from bit k_{4r-3} where r denotes the round. Assume that the initial key is:

$$K = 0011\ 1010\ 1001\ 0100\ 1101\ 0110\ 0011\ 1111 \quad (10)$$

and the plaintext be

$$x = 0010\ 0110\ 1011\ 0111. \quad (11)$$

Find the ciphertext:

1st round

$$\begin{array}{lcl}
 K = K_1 & \xrightarrow{1} & \xrightarrow{12} \quad \xrightarrow{2} \quad \xrightarrow{3} \\
 u' = x \oplus K = & 0001 & 1100 \quad 0010 \quad 0011 \\
 v^1 = 0 & 0100 & 0101 \quad 1101 \quad 0001 \\
 w' = & 0010 & 1110 \quad 0000 \quad 0001
 \end{array}$$

Arrows indicate bit shifts: 1, 12, 2, 3, 4, 5, 13, 1.

$$u^2 = w' \oplus K^2 = \dots$$

$$l: \log l. \ll l \cdot 2^l.$$