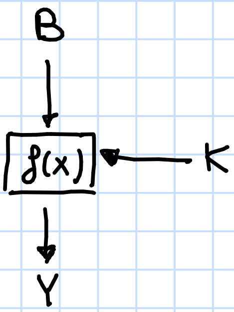
Es 1

Consider the following Feistel scheme

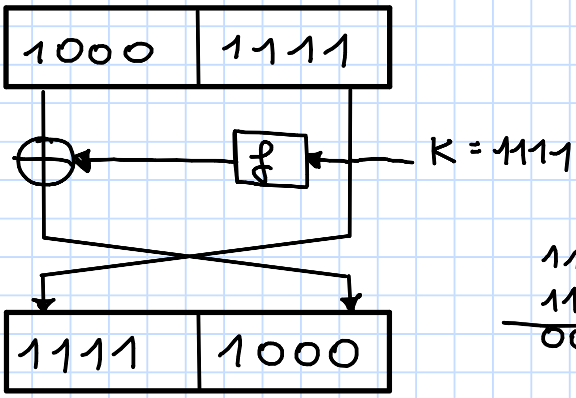


$B = 1000\ 1111$

$K = 1111$

$f(x) = x \oplus K$

Solution:



$$\begin{array}{l} 1111 \text{ XOR} \\ 1111 \ = \\ \hline 0000 \end{array}$$

$Y = 1111\ 1000$

Es. 2

Compute the value of $S_1(55)$ in DES algorithm

Here is S_1:

S_1	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0yyyy1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1yyyy0	4	1	14	8	13	6	2	11	15	12	9	$\boxed{7}$	3	10	5	0
$\boxed{\text{1yyyy1}}$	15	12	8	2	4	9	1	7	5	11	3	$\boxed{14}$	10	0	6	13

Solution

$55 = 32+16+4+2+1 = 2^5+2^4+2^2+2^1+2^0 = 1\overbrace{1011}^{\text{col } 11}1$

row 3

$S(55) = 14$

$S(54) \Rightarrow 54 = 1\overbrace{1011}^{\text{col } 11}0$

row 2

$\Downarrow$

$S_1(54) = 7$

Es 3

RSA parameters: $p=5$, $q=11$. What is a valid combination for RSA?

a) $e=12$ $M=6$

b) $e=17$ $d=33$ $M=6$ $C=41$ ✓

c) $e=11$ $d=11$ $M=6$ $C=16$

RSA encryption: $C=M^e \bmod N$ where $N=pq$ and $e \in \mathbb{Z}_{\Phi(N)}$ s.t. $\gcd(e,\Phi(N))=1$

RSA decryption: $M=C^d \bmod N$ where $d=e^{-1} \bmod \Phi(N)$

1st option: $e=12 \Rightarrow d=e^{-1} \bmod \Phi(N)$

$d=12^{-1} \bmod 40 \Rightarrow \gcd(12,40) \neq 1$ then 12 is not invertible mod 40

2nd option: $\gcd(17,40)=1$

$40=17\times2+6$ $\quad p_0=0$

$17=6\times2+5$ $\quad p_1=1$

$6=5\times1+1$ $\quad p_2=0-2 \bmod 40 \equiv 38$

$5=\ \times5+0$ $\quad p_3=1-38\times2=5$

$p_4=38-5 \equiv 33 \bmod 40$

$C=M^e \bmod N = 6^{17} \bmod 55$

$6^{17}=6^{10}\cdot6^7=6^7=6^3\cdot6^2\cdot6^2=51\cdot36\cdot36=21\cdot36\equiv41 \bmod 55$

3rd option:

$11\cdot11=121\equiv11\not\equiv1 \bmod 55$

Es. 4

DSA algorithm. Given $p = 11, q = 5, d = 4$, what is the public key?

a) $(11, 5, 9, 5)$ ✓

b) $(11, 5, 3, 5)$

c) $(11, 5, 7, 3)$

d) $(11, 5, 2, 4)$

e) $(11, 5, 4, 2)$

- We have to find a generator $\alpha \in \mathbb{Z}_p$ with $ord(\alpha) = q$, i.e an element which generates $\mathbb{Z}_q$ s.t $\alpha^q \equiv 1 \bmod p$

$\mathbb{Z}_q = \mathbb{Z}_5 = \{1, 2, 3, 4\}$

Choose 3:

$3^1 = 3$ ok!
$3^2 \equiv 4 \bmod 5$
$3^3 = 3 \cdot 3^2 = 3 \cdot 4 \equiv 2 \bmod 5$
$3^4 = 3^3 \cdot 3 = 2 \cdot 3 \equiv 1 \bmod 5$

- The private Key is $d = 4$

$\beta = \alpha^d \bmod p = 3^4 \bmod 11 = 3^2 \cdot 3^2 = 9 \cdot 9 \equiv 4 \bmod 11$

public Key is $(p, q, \alpha, \beta) = (11, 5, 3, 4)$ not in the options

Try another generator

$\alpha = 2$

$2^1 = 2$
$2^2 = 4$ ok
$2^3 \equiv 3$
$2^4 \equiv 1 \bmod 5$

$\beta = \alpha^d \bmod p = 2^4 \bmod 11 \equiv 5$

Public Key $= (11, 5, 2, 5)$ not in the options

Switch p and q $\Rightarrow p = 5, q = 11$

a) $9^1 = 9$

$9^2 = 4$

$9^3 = 3$

$9^4 = 5$

$9^5 = 1$ acceptable

$\beta = \alpha^d \bmod p = 9^4 \bmod 11 = 5$

$K_{pub} = (11, 5, 9, 5)$

b) $3^1 = 3$

$3^2 = 9$

$3^3 = 5$

$3^4 = 4$

$3^5 \equiv 1 \bmod 11$ acceptable

$\beta = 3^4 \bmod 11 = 4$

$K_{pub} = (11, 5, 3, 4)$

c) $7^1 = 7$

$7^2 = 5$

$7^3 = 2$

$7^4 = 3$

$7^5 = 10$ not acceptable

d) $2^1 = 2$

$2^2 = 4$

$2^3 = 8 = 3 \bmod 5$

$2^4 = 5$

$2^5 = 10$ not acceptable

e) $4^1 = 4$

$4^2 = 5$

$4^3 = 9$

$4^4 = 3$

$4^5 \equiv 1$ acceptable

$\beta = 4^4 \bmod 11 \equiv 3$

$K_{pub} = (11, 5, 4, 3)$