The RSA Cryptosystem

Example: Use RSA cipher with public key $n = 713 = (23)(31)\ and\ e = 43$

1) Encode the message " HELP" into their equivalents and encrypt them and
2) Decrypt the cipher text and find the original message. (DIY)

08 05 12 16

Let us next determine the corresponding ciphertext using $C = M^e\ mod\ pq$ with $e = 43$ and $pq = 713$ (values were given in the mentioned example)

H

$$8^1\ mod\ 713 = 8\ mod\ 713 = 8$$
$$8^2\ mod\ 713 = 64\ mod\ 713 = 64$$
$$8^4\ mod\ 713 = 64^2\ mod\ 713 = 531$$
$$8^8\ mod\ 713 = 531^2\ mod\ 713 = 326$$
$$8^{16}\ mod\ 713 = 326^2\ mod\ 713 = 39$$
$$8^{32}\ mod\ 713 = 39^2\ mod\ 713 = 95$$

$$\begin{aligned}\underline{8^{43}\ mod\ 713} &= (8^{32} \cdot 8^8 \cdot 8^2 \cdot 8^1)\ mod\ 713 \qquad 43 = 32 + 8 + 2 + 1 \\ &= (8^{32}\ mod\ 713 \cdot 8^8\ mod\ 713 \cdot 8^2\ mod\ 713 \cdot 8^1\ mod\ 713)\ mod\ 713 \\ &= (95 \cdot 326 \cdot 64 \cdot 8)\ mod\ 713 \\ &= 15,856,640\ mod\ 713 \\ &= 233\end{aligned}$$

E

$$5^1\ mod\ 713 = 5\ mod\ 713 = 5$$
$$5^2\ mod\ 713 = 25\ mod\ 713 = 25$$
$$5^4\ mod\ 713 = 25^2\ mod\ 713 = 625$$
$$5^8\ mod\ 713 = 625^2\ mod\ 713 = 614$$
$$5^{16}\ mod\ 713 = 614^2\ mod\ 713 = 532$$
$$5^{32}\ mod\ 713 = 532^2\ mod\ 713 = 676$$

$$\begin{aligned}\underline{5^{43}\ mod\ 713} &= (5^{32} \cdot 5^8 \cdot 5^2 \cdot 5^1)\ mod\ 713 \\ &= (5^{32}\ mod\ 713 \cdot 5^8\ mod\ 713 \cdot 5^2\ mod\ 713 \cdot 5^1\ mod\ 713)\ mod\ 713 \\ &= (676 \cdot 614 \cdot 25 \cdot 5)\ mod\ 713 \\ &= 51,883,000\ mod\ 713 \\ &= 129\end{aligned}$$

L

$$12^1 \; mod \, 713 = 12 \; mod \, 713 = 12$$
$$12^2 \; mod \, 713 = 144 \; mod \, 713 = 144$$
$$12^4 \; mod \, 713 = 144^2 \; mod \, 713 = 59$$
$$12^8 \; mod \, 713 = 59^2 \; mod \, 713 = 629$$
$$12^{16} \; mod \, 713 = 629^2 \; mod \, 713 = 639$$
$$12^{32} \; mod \, 713 = 639^2 \; mod \, 713 = 485$$

$$\begin{aligned}\underline{12^{43} \; mod \, 713} &= (12^{32} \cdot 12^8 \cdot 12^2 \cdot 12^1) \; mod \, 713 \\ &= (12^{32} \; mod \, 713 \cdot 12^8 \; mod \, 713 \cdot 12^2 \; mod \, 713 \cdot 12^1 \; mod \, 713) \; mod \, 713 \\ &= (485 \cdot 629 \cdot 144 \cdot 12) \; mod \, 713 \\ &= 527,152,320 \; mod \, 713 \\ &= 48\end{aligned}$$

P

$$16^1 \; mod \, 713 = 16 \; mod \, 713 = 16$$
$$16^2 \; mod \, 713 = 256 \; mod \, 713 = 256$$
$$16^4 \; mod \, 713 = 256^2 \; mod \, 713 = 653$$
$$16^8 \; mod \, 713 = 653^2 \; mod \, 713 = 35$$
$$16^{16} \; mod \, 713 = 35^2 \; mod \, 713 = 512$$
$$16^{32} \; mod \, 713 = 512^2 \; mod \, 713 = 473$$

$$\begin{aligned}\underline{16^{43} \; mod \, 713} &= (16^{32} \cdot 16^8 \cdot 16^2 \cdot 16^1) \; mod \, 713 \\ &= (16^{32} \; mod \, 713 \cdot 16^8 \; mod \, 713 \cdot 16^2 \; mod \, 713 \cdot 16^1 \; mod \, 713) \; mod \, 713 \\ &= (473 \cdot 35 \cdot 256 \cdot 16) \; mod \, 713 \\ &= 67,809,280 \; mod \, 713 \\ &= 128\end{aligned}$$

We then obtain the encrypted message by replacing each digit by the corresponding ciphertext:

$$233 \; 129 \; 048 \; 128$$

8.2 Solving Linear Recurrence Relations

Problem 13: Let f_n be the Fibonacci numbers, i.e., $f_0 = f_1 = 1$ and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$. Define a_n as

$$a_n = \frac{f_n}{f_{n-1}}, \qquad \text{for } n \in \mathbf{N}.$$

Give a recurrence relation to compute a_n and solve the relation.

Hint: Assume that a_n converges to r as $n \to \infty$.

Problem 14: Solve the following recurrence relation:

$$\begin{cases} a_0 = 0, \\ a_1 = -1, \\ a_n - 7a_{n-1} + 12a_{n-2} = 0 \quad \text{for } n \geq 2. \end{cases}$$

Problem 15: Solve the following recurrence relation:

$$\begin{cases} a_1 = 1, \\ a_2 = 1, \\ a_n + 2a_{n-1} - 15a_{n-2} = 0 \quad \text{for } n \geq 3. \end{cases}$$

Problem 16: Solve the following recurrence relation:

$$\begin{cases} a_0 = 2, \\ a_1 = 0, \\ -2a_n + 18a_{n-2} = 0 \quad \text{for } n \geq 2. \end{cases}$$

Solution 14: Let $a_0 = 0, a_1 = -1$, and for $n \geq 2,\ a_n - 7a_{n-1} + 12a_{n-2} = 0$.

Step 1: The associated characteristic equation is $r^2 - 7r + 12 = 0$ and its two roots are $r = 3$ and $r = 4$.

Step 2: We note that (i) the nonhomogeneous part is 0 and (ii) all characteristic roots are distinct. Thus, the general solution to the given recurrence equation is

$$a_n = A3^n + B4^n.$$

Step 3: We use the initial conditions to solve the following equations for the unknown constants A and B.

$$\left.\begin{array}{ll} n = 0: & 0 = A + B, \\ n = 1: & -1 = 3A + 4B. \end{array}\right\} \implies A = 1,\ B = -1.$$

Therefore,

$$a_n = 3^n - 4^n, n \geq 0.$$

Solution 15: Let $a_1 = 1, a_2 = 1$, and for $n \geq 3, a_n + 2a_{n-1} - 15a_{n-2} = 0$.

Step 1: The associated characteristic equation is $r^2 + 2r - 15 = 0$ and its two roots are $r = -5$ and $r = 3$.

Step 2: We note that (i) the nonhomogeneous part is 0 and (ii) all characteristic roots are distinct. Thus, the general solution is

$$a_n = A(-5)^n + B3^n.$$

Step 3: We use the initial conditions to solve the following equations for the unknown constants A and B. [Note: n starts from 1.]

$$\left.\begin{array}{ll} n = 1: & 1 = -5A + 3B \\ n = 2: & 1 = 25A + 9B \end{array}\right\} \implies A = -\frac{1}{20},\ B = \frac{1}{4}.$$

Therefore,

$$a_n = -\frac{1}{20} \times (-5)^n + \frac{1}{4} \times 3^n = \frac{1}{4}(-5)^{n-1} + \frac{1}{4} \times 3^n,\ n \geq 1.$$

Course Incharge : Muhammad Jamilusmani