RSA Crypto Algorithm

Key Generation (Receiver Side)

1.

$$
p = 17 \\
q = 11
$$

2.

$$
n = p \cdot q \\
n = 17 \cdot 11 \\
n = 187
$$

3.

$$
\lambda(n) = lcm(p-1, q-1) \\
\lambda(187) = lcm(16, 10) \\
\lambda(187) = 80
$$

4.

$$
(\gcd(80, e) = 1) \;\&\, \&(1 < e < 80) \\
e = 3
$$

5.

$$
d = e^{-1} \mod \lambda(n) \\
d = 3^{-1} \mod 80
$$

- Extended Euclidean Algorithm:

q	a	b	r	t_1	t_2	$t = t_1 - t_2 \cdot q$
26	80	3	2	0	1	-26
1	3	2	1	1	-26	27

$$
r = 1 \Rightarrow d = t = 27 \mod 80 = 27
$$

6.

در الگوریتم rsa هر فرد دو کلید دارد که یک کلید عمومی است و آنرا در اختیار همه می گذارد، کلید دیگر خصوصی است و باید پیش خود شخص مخفی بماند. افراد دیگر با استفاده از کلید عمومی که دارند می توانند پیام خود را رمز کنند و به شخص مورد نظر بفرستند و آن شخص با استفاده از کلید خصوصی خود می تواند پیام را رمزگشایی کند و هیچ کس به جز او نمی تواند این پیام را رمزگشایی کند چون کلید باز کردن را فقط خود شخص دارد.

$$
\textbf{privateKey} = \{d, n\} = \{27, 187\} \\
\textbf{publicKey} = \{e, n\} = \{3, 187\}
$$

با عوض کردن جای کلید عمومی و خصوصی الگوریتم همچنان کار می کند:

$$m = (m^e)^d = (m^d)^e \mod n$$

اما، در این الگوریتم کلید خصوصی باید بزرگ باشد تا قابل حدس یا حمله نباشد و از طرفی کلید عمومی باید کوچک باشد تا هزینه رمزکردن کم باشد. بنابرین الگوریتم با عوض کردن جای کلید ها همچنان کار می کند اما از لحاظ امنیتی مشکل دارد و کاربردی نیست.

Encryption (Sender Side)

Message: $m = 13$
Ciphertext: $c = ?$

$$c = m^e \mod n$$
$$c = 13^3 \mod 187$$
$$c = 140$$

Decryption (Receiver Side)

Ciphertext: $c = 140$
Message: $m = ?$

$$m = c^d \mod 187$$
$$m = 140^7 \mod 187$$
$$m = (140^1 \cdot 140^2 \cdot 140^4) \mod 187$$
$$140 \mod 187 = -47$$
$$140^2 \mod 187 = -47 * -47 = 152 = -35$$
$$140^4 \mod 187 = -35 \cdot -35 = 103 = -84$$
$$m = (140 \cdot -35 \cdot -84) \mod 187$$
$$m = 13$$

Diffie-Helman

1.

$$p = 23$$

2.

با استفاده از کد زیر مولد را پیدا می کنیم:

```python
p = 23
for i in range(1, p): # [1, p-1]
    visited = [False] * p
    trace = []
    k = 1
    counter = 0
    while True:
        if counter == p-1:
            break
        if visited[k] == True:
            break
        visited[k] = True
        k = (k * i) % p
        if k == 0:
            break
        counter += 1
        trace.append(k)
    if counter == p-1:
        print('generator: ', i)
        print(trace)
        break
```

```
generator:  5
[5, 2, 10, 4, 20, 8, 17, 16, 11, 9, 22, 18, 21, 13, 19, 3, 15, 6, 7, 12, 14, 1]
```

3.

در الگوریتم Diff-Hellman باید سعی کنیم احتمال وجود تمام اعداد را در متن رمز شده باقی بگذاریم تا بیشترین میزان امنیت را داشته باشیم اگر مقدار p مولد نباشد آنگاه حمله کننده می تواند آزمون های بسیار کمتری نسبت به حالت مولد بودن آن انجام دهد و رمز ما را بشکند.

4.

$$\alpha = 29$$
$$\beta = 31$$

5.

$$g^{\alpha} \mod p = 5^{29} \mod 23$$
$$= 5^{(11101)_2} \mod 23$$
$$5 \mod 23 = 5$$
$$5^2 \mod 23 = 2$$
$$5^4 \mod 23 = 4$$
$$5^8 \mod 23 = 16$$
$$5^16 \mod 23 = 3$$
$$5^{29} \mod 23 = 5 \cdot 4 \cdot 16 \cdot 3 = 17$$

$$g^{\beta} \mod p = 5^{31} \mod 23$$
$$= 5^{(11111)_2} \mod 23$$

$$
\begin{gathered}
5 \mod 23 = 5 \\
5^2 \mod 23 = 2 \\
5^4 \mod 23 = 4 \\
5^8 \mod 23 = 16 \\
5^{16} \mod 23 = 3 \\
5^{31} \mod 23 = 5 \cdot 2 \cdot 4 \cdot 16 \cdot 3 = 11
\end{gathered}
$$

6.

$$
\begin{gathered}
(g^\alpha)^\beta = 17^{31} \mod 23 \\
= 17^{(11111)_2} \mod 23 \\
17 \mod 23 = -6 \\
17^2 \mod 23 = 13 \\
17^4 \mod 23 = 8 \\
17^8 \mod 23 = 18 \mod 23 = -5 \\
17^{16} \mod 23 = 2 \\
17^{(11111)_2} \mod 23 = -6 \cdot 13 \cdot 8 \cdot -5 \cdot 2 = 7
\end{gathered}
$$

$$
\begin{gathered}
(g^\beta)^\alpha = 11^{29} \mod 23 \\
11 \mod 23 = 11 \\
11^2 \mod 23 = 6 \\
11^4 \mod 23 = 13 \\
11^8 \mod 23 = 8 \\
11^{16} \mod 23 = 18 = -5 \\
11^{29} \mod 23 = 11^{16} \cdot 11^8 \cdot 11^4 \cdot 11^1 \mod 23 \\
= -5 \cdot 8 \cdot 13 \cdot 11 \mod 23 \\
= 7
\end{gathered}
$$

$$7 = 7 :)$$