$P = 11$
$Q = 27, 29$

# I. Miller-Rabin

$P = 27 d = 13 S = 1$
$a = 2, 7, 11...$

1. $a^d \equiv 1 \mod P$
2. $a^{d*2^r} \equiv P - 1 \mod P$

$2^{13} \equiv \mod 27$
toBinary(13) = 1101

$2^{2^0} \equiv 2$
$2^{2^1} \equiv 4 \mod 27$
$2^{2^2} \equiv 16$
$2^{2^3} \equiv 13$

$2 \cdot 16 \cdot 13 \mod 27 \rightarrow 11$

$2^{13 \cdot 2^0} \mod 27$

$d = \frac{28}{2^1} = 14$
$d = \frac{28}{2^2} = 7$
$7^7 \mod 29$
toBinary(7) = 111

$7^{2^0} \equiv 7$
$7^{2^1} \equiv 20 \mod 29$
$7^{2^2} \equiv 23$

$7 \cdot 20 \cdot 23 \mod 29$
1

$7^{7 \cdot 2^0} \equiv 1$
$7^{7 \cdot 2^1} \equiv 1 \mod 29$
$7^{7 \cdot 2^2} \equiv 1$

## II.

P = 11 Q = 27, 29
n = 11 * 29 = 319

$\phi(n) = (p \cdot 1) \cdot (Q \cdot 1) = 280$
{15, 21, 17, 30}

$(280, 17) = 1$

| k | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| - | 280 | 17 | 8 | 1 | 0 |
| - | - | 16 | 2 | 8 | |
| xk | 1 | 0 | 1 | 2 | |
| yk | 0 | 1 | 16 | 33 | |

$X = xk \cdot (-1)^k$
$Y = yk \cdot (-1)^{k+1}$

$X = 2 \cdot (-1)^3 = -2$
$Y = 33 \cdot (-1)^4 = 33$
$\Rightarrow d = 33$

## III.

$m = 15$

$15^7 \mod n$

toBinary(17) = 10001

1 - $2^{15^0} \equiv 15$
0 - $2^{15^1} \equiv 225$

0 - $2^{15^2} \equiv 223 \mod 319$
0 - $2^{15^3} \equiv 284$
1 - $2^{15^4} \equiv 268$

$15 \cdot 268 \mod 319 \rightarrow c = 192$

---

# IV. Kínai maradéktétel

$c^d \mod n$

$\sum c_i \cdot y_i \cdot M_i \mod M$
$P = 11$
$Q = 29$
$C = 192$
$d = 33$

$M = P \cdot Q$
$M_1 = \frac{M}{P} = Q$
$M_2 = \frac{M}{Q} = P$

$C_1 = C^{(d \mod P-1)} \mod P$
$C_2 = C^{(d \mod Q-1)} \mod Q$

$M_1 = \frac{M}{P} = Q$
$M_2 = \frac{M}{Q} = P$

$C_1 = 192^{(33 \mod 10)} \mod 11 \rightarrow 4$
$C_2 = 192^{(33 \mod 28)} \mod 29 \rightarrow 15$

$1 = y_1 \cdot M_1 + y_2 \cdot M_2$

$1 = y_1 \cdot 29 + y_2 \cdot 11$

| k | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| - | 29 | 11 | 7 | 4 | 3 | 1 | 0 |
| - | - | 2 | 1 | 1 | 1 | 3 | |
| y1 | 1 | 0 | 1 | 1 | 2 | 3 | |
| y2 | 0 | 1 | 2 | 3 | 5 | 8 | |

$y_1 = 3 \cdot (-1)^k$
$y_2 = 3 \cdot (-1)^{k+1}$

$y_1 = 3 \cdot (-1)^5 = -3$
$y_2 = 8 \cdot (-1)^6 = 8$

$4 \cdot -3 \cdot 29 + 15 \cdot 8 \cdot 11 \mod 319$
$\Rightarrow 15 \mod 319$