Ex^m

$p = 5 \qquad q = 11$

Key generation

Public keys: n, e 55 and 3

Private key d 27

Encoding:

A	B	C	D	.	.		Z
0	1	2	3	–	.	.	25

HELLO

H $\rightarrow$ 7

Encoding for H.

$$c \equiv m^e \bmod n$$

$$c \equiv 7^3 \bmod 55$$

$$\equiv 13 \bmod 55$$

encrypted message is $13 \rightarrow N$

Decryption: Bob received N $\rightarrow$ 13

$$M \equiv c^d \bmod n$$

$$\equiv 13^{27} \bmod 55$$

$$\equiv \underbrace{13^2 \cdot 13^2 \cdot \cdots 13^2}_{13} \cdot 13$$

$$\equiv 4 \cdot 4 \cdots 4 \cdot 13$$

$$\equiv 64 \cdot 64 \cdot 64 \cdot 64 \cdot 4 \cdot 13$$

$$\equiv 9 \cdot 9 \cdot 9 \cdot 9 \cdot 4 \cdot 13$$

$$\equiv 7 \bmod 55$$

$7 \rightarrow H$.

$13^2 \bmod 55$ 169

Why RSA algorithm is correct?

we need to show that $c^d \bmod n$ is m.

$$c^d \equiv (m^e)^d \bmod n$$
$$\equiv m^{ed} \bmod n.$$

we have, $ed \equiv 1 \bmod K$

$\Rightarrow ed = tK + 1$

where t is any integer.

$$c^d \equiv m^{ed} \bmod n$$
$$\equiv m^{tK+1} \bmod n$$
$$\equiv m^{t(p-1)(q-1)} \bmod n$$

$$c^d \equiv m^{t(p-1)(q-1)+1} \mod pq$$

$$\equiv m \cdot m^{t(p-1)(q-1)} \mod pq$$

$$m\left(m^{(p-1)}\right)^{t(q-1)} \mod pq$$

$$m \cdot \left(m^{(q-1)}\right)^{t(p-1)} \mod pq$$

Fermats little theorem.

$$m^{p-1} \equiv 1 \mod p$$

$$m^{q-1} \equiv 1 \mod q.$$

$$c^d \equiv m \cdot \left(m^{p-1}\right)^{t(q-1)} \mod p$$

$$= m$$

$$c^d \equiv m\left(m^{q-1}\right)^{t(p-1)} \mod q$$

$$= m$$

we have,

$$\left.\begin{aligned} c^d &\equiv m \mod p \\ c^d &\equiv m \mod q \end{aligned}\right\}$$

By chinese remainder theorem
The system has a unique solution mod pq.

$$c^d \equiv m \mod pq$$