$p = 13$

$g = 7$

Alice

$a \xleftarrow{\$} \{2 \dots 11\}$

$a = 4$

$A = 7^4 \bmod 13$

$= 7^2 . 7 . 7 \bmod 13$

$= 10 . 7 . 7 . \bmod 13$

$= 5 . 7 . \bmod 13$

$= 9$

Bob

$b \xleftarrow{\$} \{2, \dots 12\}$

$b = 5$

$B = 7^5 \bmod 13$

$= 9 . 7 . \bmod 13$

$= 11$

Alice

$a = 4$

$B = 11$

$B^a \bmod 13$

$= \boxed{11^4 \bmod 13}$

$= (7^5)^4 \bmod 13$

$= 7^{20} \bmod 13$

$= 3$

Bob

$b = 5$

$A = 9$

$A^b \bmod 13$

$= 9^5 \bmod 13$

$= (7^4)^5 \bmod 13$

$= 7^{20} \bmod 13$

$= 3$

$g^a \bmod p \longrightarrow a$

classical.

No "good" algorithm is known

1 . . . pq

number of int. relatively prime to pq

$pq - p - q + 1$ pq.

$= p(q-1) - (q-1)$

$= (p-1)(q-1)$

$\phi(n) = (p-1)(q-1)$

Encrypt(m, 7, 55)

$m = 17.$

$C = m^e \bmod n$

$= 17^7 \bmod 55.$

$= 8$

decrypt(c, d, n)

$m = c^d \bmod n.$

$$= 8^{23} \mod 55$$

$$= 2^{69} \mod 55$$

$$= \left(2^{15}\right)^4 \cdot 2^9 \mod 55$$

$$= \left(2^{15} \mod 55\right)^4 \cdot 2^9 \mod 55$$

$$= 1 \cdot 2^9 \mod 55$$

$$= 1 \cdot 17 \mod 55$$

$$= 17$$

Square & multiply

Sign(m, d, N)

$$\sigma = H(m)^d \bmod N$$

Verify

(m, σ, e, N)

$$\sigma^e \bmod N \stackrel{?}{=} H(M)$$

MySign (m, d, n)

$\sigma = m^d \bmod n$

$\sigma = H(m)^d \bmod N$

MyVerify (m, σ, n)

if $\sigma^e \bmod n = m$

o/p accept

else o/p reject.