RSA Algorithm

Euclidean Alg.

Two positive integers a and b.

$a = bq + r \quad 0 \le r < b$

$b = r(q_1) + r_1 \quad 0 \le r_1 < r$

$r = r_1(q_2) + r_2 \quad 0 \le r_2 < r_1$

⋮

continue until remainder is zero

$r_{i-2} = r_{i-1} q_i + r_i \quad 0 \le r_i < r_{i-1}$

$r_{i-1} = r_i q_{i+1} + 0$

The last nonzero remainder is the gcd. So, $\gcd(a,b) = r_i$

Example: Input 34,55

$55 = 34(1) + 21$

$34 = 21(1) + 13$

$21 = 13(1) + 8$

$13 = 8(1) + 5$

$8 = 5(1) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

$\gcd(55, 34) = 1$

RSA Key Selection

step-1: $p = 11, q = 5, n = p \times q; \; n = 11 \times 5 = 55$

step-2: Calculate the totient of RSA modules.

$$\varphi(n) = (p-1)(q-1)$$
$$= (11-1)(5-1) = 40$$

* The totient function/ Euler's totient function, is defined as the number of positive integers that are positively prime to (i.e., do not contain any factor in common with, where 1 is counted as being relatively prime to all numbers.

step-3: select a number, e, that is relative prime to the totient and is $1 < e < \varphi(n)$. (e is public)

So, 3, 7, 9, 11, 13, 17 -----.

We have chosen, $e = 7$ co-prime of $\varphi(n)$

private				public	
p	q	φ(n)	d	n	e
11	5	40	23	55	7

Now encryption and decryption

Alice

message: HIDE

$c = p^e \bmod n$

First encrypt H, numerical representation of H is 7

So, $p = 7$

$c = 7^7 \bmod 55$

$= 28$ (is the ciphertext of H)

Similarly

for $I = 8^7 \bmod 55 = 2$

$D = 3^7 \bmod 55 = 42$

$E = 4^7 \bmod 55 = 49$

Bob

ciphertext: 28, 2, 42, 49

$p = c^d \bmod n$

$28 = 28^{23} \bmod 55 = 7 = H$ [see Fast exponential modular arithmetic]

$2 = 2^{23} \bmod 55 = 8 = I$

$42 = 42^{23} \bmod 55 = 3 = D$

$49 = 49^{23} \bmod 55 = 4 = E$

So, our plaintext = HIDE

e, n → public
φ, d → secret

Extended Eucl. Alg. useful when a and b are coprime (or gcd is 1)

Step-4: Calculating d using the following equation.

$$d \times e = 1 \bmod \varphi(n) \quad (\text{or } d \times e \bmod \varphi(n) = 1)$$
$$d(7) = 1 \bmod 40 \quad (\text{or } d(7) \bmod 40 = 1)$$

Use Extended Euclidean Alg. to solve this:

$$40x + 7y = 1$$

$40 = 5(7) + 5$
$7 = 1(5) + 2$
$5 = 2(2) + 1$
$2 = 2(1) + 0$

we stop at the last non-zero remainder, then use the extended Euclidean Alg.

Back substitute:

$5 = 2(2) + 1$
$1 = 5 - 2(2)$
$1 = 5 - 2(7 - 1(5))$
$= (5) - 2(7) + 2(5)$
$= 3(5) - 2(7)$
$= 3(40 - 5(7)) - 2(7)$
$= 3(40) - 15(7) - 2(7)$
$= 3(40) - 17(7)$

$\therefore d = 40 - 17 = 23$. (if negative)

if 17 was positive then d = 17