RSA

Sender, Alice

Recipient, Bob

Eavesdropper, Eve

Bob

(1) Choose primes p, q, r

(2) $N = pqr$

(3) Find e coprime with $(p-1)(q-1)(r-1)$

(4) Compute $d \equiv e^{-1} \bmod (p-1)(q-1)(r-1)$

(5) Broadcast (N, e)

Alice

(6) Wants to send x

(7) Compute $E(x) = x^e \bmod N$

(8) Broadcast $E(x)$

(9) $D(E(x)) = (E(x))^d \bmod N$

$\equiv x^{ed} \bmod N$

$$x^{ed} \equiv x \bmod N$$

$x^{k(p-1)(q-1)(r-1)+1} - x \equiv 0 \bmod p$

Proof of

Lemma 1: $x \cdot x^{k(p-1)(q-1)} \equiv x \cdot 1^{k(q-1)} \equiv x \cdot 1 \equiv x \bmod p$

$\equiv x^{k(p-1)(q-1)+1} \equiv x \bmod p$

$\Rightarrow x^{k(p-1)(q-1)+1} - x \equiv 0 \bmod p$

$\Rightarrow p \mid (x^{k(p-1)(q-1)+1} - x)$ ... (i)

$q \mid (x^{k(p-1)(q-1)+1} - x)$ ... (ii)

$\Rightarrow pq \mid (x^{k(p-1)(q-1)+1} - x)$

$\Rightarrow (x^{k(p-1)(q-1)+1} - x) \equiv 0 \bmod pq$

$\Rightarrow x^{k(p-1)(q-1)+1} \equiv x \bmod pq$ ↑?

$ed \equiv k(p-1)(q-1) + 1 \equiv 1 \mod (p-1)(q-1)$

$\Rightarrow d \equiv e^{-1} \mod (p-1)(q-1)$ $\because \gcd(e, (p-1)(q-1)) = 1$

$\blacksquare$

$p = 3 \quad q = 5$

$pq = 15$

$\gcd(14, 15) = 1$

$(p-1)(q-1) = 8$

$\gcd(14, 8) = 2$

Suppose we have an RSA scheme with public keys (N, e) where $N = pq$ and e which is relatively prime to $(p-1)(q-1)$ and private key d. We have the encryption function: $E(m) = m^e \pmod{N}$ and decyption function $D(c) = c^d \pmod{N}$.

(a) Show that $E(ab \pmod{N}) = E(a)E(b) \pmod{N}$

(b) Alice suspects that Bob might have misplaced his RSA private key. So she asks him to decrypt a ciphertext to prove to her that he still has it. Bob suspects there is something fishy about Alice's claim, but he believes her anyway, and is willing to decrypt the ciphertext for Alice. Assume Alice randomly generates a number $r \mod N$. She also encrypts r to get $c = E(r)$. Assume $r \neq 0 \pmod{N}$.

It turns out Alice has an ulterior motive: She has intercepted a ciphertext $E(a)$ that Eve sent Bob and is dying to decrypt it to recover the message a. Show how Alice can use Bob's help to recover the message a without just sending $E(a)$. Bob is not dumb, if he decrypts his own message, he'll know what's up!

1. Alice and Bob are having a hard time finding new prime numbers, so they decide to share one. Alice uses primes p and q (so that $N = pq$) and some e relatively prime to $(p-1)(q-1)$; Bob uses primes q and r and some other e' relatively prime to $(q-1)(r-1)$. Is this scheme secure?

Efficient

Addition
Multiplication
Division
Finding mod inverse
Modular exponentiation
Finding gcd

Inefficient

Factorization

N'

$N = pq$, $N' = qr$

$\gcd(N, N') = q$

$r = \frac{N'}{q}$

$p = \frac{N}{q}$

$4^{-1} \bmod 7$

8. RSA with three primes, two exponents, and a glitch (15 pts)

Suppose you have three distinct primes p, q, r and positive natural numbers e_1 and e_2 that are both coprime with $p-1, q-1$, and $r-1$.

Suppose further that x is a natural number from $1, 2, \ldots, pqr-1$. Let $y_1 = x^{e_1} \bmod pqr$ and $y_2 = x^{e_2} \bmod pqr$ be two different encryptions of x.

There was a glitch and you lose both y_1 and y_2. Suppose you only have access to $y_p = y_1 \bmod p$ and $y_q = y_1 \bmod q$ from the first encryption, and $y_r = y_2 \bmod r$ from the second encryption.

Give an explicit way to recover x from these three numbers y_p, y_q, y_r, given knowledge of p, q, r, e_1, e_2. Describe all computations that you would have to do. You may invoke egcd as a subroutine freely, as well as standard mod operations of addition, multiplication, and exponentiation.

(HINT: You might want to recover x_p, x_q, x_r first.)

$a^{p-1} \equiv 1 \bmod p$

$x_p = x \bmod p$
$x_q = x \bmod q$
$x_r = x \bmod r$

(1) Paraphrase

$y_p \equiv y_1 \bmod p \equiv (x^{e_1} \bmod pqr) \bmod p \equiv x^{e_1} \bmod p$

$y_q \equiv y_1 \bmod q \equiv (x^{e_1} \bmod pqr) \bmod q \equiv x^{e_1} \bmod q$

$y_r \equiv y_2 \bmod r \equiv (x^{e_2} \bmod pqr) \bmod r \equiv x^{e_2} \bmod r$

Let $a = x^{e_1} \bmod pqr$
$\Rightarrow a = kpqr + x^{e_1} \bmod p$
$(x \bmod p) \bmod pqr$

$x = 14$
$x \bmod 2 = 0$
$(x \bmod 2) \bmod 30 = 0 \neq 14 \bmod 30$

(2) Find inverses

$d_p = e_1^{-1} \bmod (p-1)$

$d_q = e_1^{-1} \bmod (q-1)$

$d_r = e_2^{-1} \bmod (r-1)$

$y_p^{d_p} \bmod p$

$= x^{e_1 d_p} \equiv x^{1+k(p-1)} \bmod p$ $\quad \because d_p \cdot e_1 \equiv 1 \bmod (p-1)$
$\Rightarrow e_1 d_p = k(p-1)+1$

$= x(x^{(p-1)})^k \bmod p$

$= x(1)^k \bmod p$ FLT

$= x \bmod p = x_p$

Repeat for q & r to get x_q, x_r.

(3) CRT

$x \equiv x_p \bmod p$
$x \equiv x_q \bmod q$
$x \equiv x_r \bmod r$

$x = x_p qr[(qr)^{-1} \bmod p]$
$+ x_q pr[(pr)^{-1} \bmod q]$
$+ x_r pq[(pq)^{-1} \bmod r]$

Have: $x^{e_1} \bmod p$ $\qquad x^{e_1 d}$

Want: $x \bmod p$

$x^{(p-1)+1} = x \bmod p$

$e_1 d = k(p-1) + 1 \bmod (p-1)$

$= 1$

$d = e_1^{-1} \bmod (p-1)$

$e_1 d \equiv 1 \bmod (p-1)$