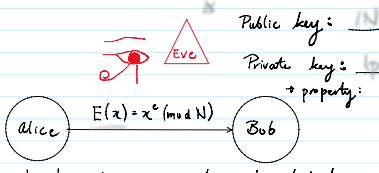
Dis 3B: RSA

Tuesday, July 7, 2020 12:24 AM

a Visual Explanation: RSA



Public key: (N, e)

Private key: $(p, q, d = e^{-1} \pmod{(p-1)(q-1)})$

→ property:

wishes to send message x to Bob

decrypts what he receives (i.e. $E(x)$) via $D(y) = y^d \pmod N$

⇒ Bob ends up with $D(E(x))$ if RSA works, $\_\_\_\_ = \_\_\_\_$

1 RSA Warm-Up

Consider an RSA scheme with modulus $N = pq$, where p and q are distinct prime numbers larger than 3.

public key: (N, e)
private key: $(p, q, d = e^{-1} \pmod{(p-1)(q-1)})$
$E(x) = x^e \pmod N$
$D(y) = y^d \pmod N$

(a) What is wrong with using the exponent $e = 2$ in an RSA public key?

$\gcd(e, (p-1)(q-1)) \neq 1$

(b) Recall that e must be relatively prime to $p-1$ and $q-1$. Find a condition on p and q such that $e = 3$ is a valid exponent.

$\gcd(3, p-1) = 1$

$p-1 \not\equiv 1 \pmod 3$

$p-1 \not\equiv 2 \pmod 3$

$\Rightarrow p \equiv 3 \equiv 0 \pmod 3$

$p = 3$

$p = 2 \pmod 3$ ... p is prime

same for q

(c) Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

$(N, e) = (pq, 3)$

$= (85, 3)$

(d) What is the private key?

$d = e^{-1} \pmod{(p-1)(q-1)}$

Type solns to c,d,e together into chat

$3^{-1} \pmod{64}$

$= 43$

(e) Alice wants to send a message $x = 10$ to Bob. What is the encrypted message $E(x)$ she sends using the public key?

$E(x) = x^e \pmod N = 10^3 \pmod{85}$

$\equiv 1000 \pmod{85}$

$\equiv 65$

(f) Suppose Bob receives the message $y = 24$ from Alice. What equation would he use to decrypt the message? What is the decrypted message?

$D(y) = y^{43} \pmod N =$

$x = 24^{43} \pmod{85}$

CRT

$x \equiv 24^{43} \pmod{17}$

$x \equiv 24^{43} \pmod 5$

$x \equiv 7^{43} \pmod{17}$

$x \equiv (-1)^{43} \pmod 5$

$x \equiv -1 \pmod 5$

CRT to get $x \pmod{17 \times 5}$

$x \equiv a_1 \pmod{m_1}$

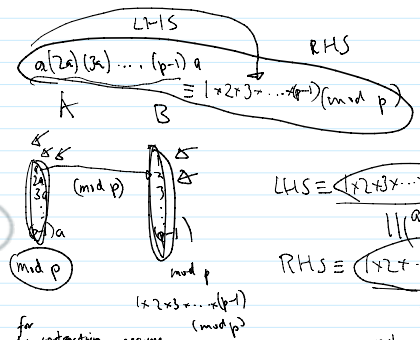
$x \equiv a_2 \pmod{m_2}$

Theorem 8.2: [Fermat's Little Theorem] For any prime p and any $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \bmod p$.

$a^{p-1} \equiv 1 \pmod p$ $\quad \gcd(a, p) = 1$

$D(E(x)) = x$?

FLT...



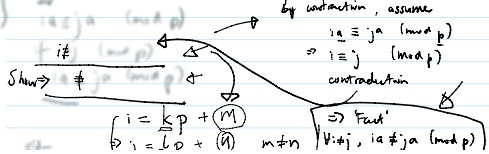
$a, b \in \mathbb{Z}$ for $a^{-1} \pmod b$ need $\gcd(a, b) = 1$

$LHS \equiv \underbrace{1 \times 2 \times 3 \times \cdots \times (p-1)}_{a^{p-1}}$

$RHS \equiv 1 \times 2 \times \cdots \times (p-1) \pmod p$

$\gcd(a, p) = 1$

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



Proof of Theorem 9.1. To prove the statement, we have to show that

$$(x^e)^d = x \bmod N \qquad \text{for every } x \in \{0, 1, \ldots, N-1\}. \tag{4}$$

Let's consider the exponent, which is ed. By definition of d, we know that $ed \equiv 1 \bmod (p-1)(q-1)$; hence we can write $ed = 1 + k(p-1)(q-1)$ for some integer k, and therefore

$$x^{ed} - x = x^{1+k(p-1)(q-1)} - x = x(x^{k(p-1)(q-1)} - 1). \tag{5}$$

Looking back at equation (4), our goal is to show that this last expression in equation (5) is equal to 0 mod N

$$(x^e)^d = x \bmod N \qquad \text{for every } x \in \{0,1,\ldots,N-1\}. \tag{4}$$

Let's consider the exponent, which is ed. By definition of d, we know that $ed \equiv 1 \bmod (p-1)(q-1)$; hence we can write $ed = 1 + k(p-1)(q-1)$ for some integer k, and therefore

$$x^{ed} - x = x^{1+k(p-1)(q-1)} - x = x(x^{k(p-1)(q-1)} - 1). \tag{5}$$

Looking back at equation (4), our goal is to show that this last expression in equation (5) is equal to 0 mod N for every x.

Now we claim that the expression $x(x^{k(p-1)(q-1)} - 1)$ in (5) is divisible by p. To see this, we consider two cases:

Case 1: *x is not a multiple of p.* In this case, since $x \neq 0 \bmod p$, we can use Fermat's Little Theorem to deduce that $x^{p-1} = 1 \bmod p$, and hence $x^{k(p-1)(q-1)} - 1 = 0 \bmod p$, as required.

Case 2: *x is a multiple of p.* In this case the expression in (5), which has x as a factor, is clearly divisible by p.

By an entirely symmetrical argument, $x(x^{k(p-1)(q-1)} - 1)$ is also divisible by q. Therefore, it is divisible by both p and q, and since p and q are primes it must be divisible by their product, $pq = N$. But this implies that the expression is equal to 0 mod N, which is exactly what we wanted to prove. □

2 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p, q, r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod N$.

3 RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(N_1, e), \ldots, (N_t, e)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

(a) Suppose Eve sees the public keys $\langle p_1 q_1, 7\rangle$ and $\langle p_1 q_2, 7\rangle$ as well as the corresponding transmissions. Can Eve use this knowledge to break the encryption? If so, how? Assume that Eve cannot compute prime factors efficiently. Think of p_1, q_1, q_2 as massive 1024-bit numbers. Assume p_1, q_1, q_2 are all distinct and are valid primes for RSA to be carried out.

(b) The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $\langle p_1 q_1, 3\rangle$, $\langle p_2 q_2, 3\rangle$, and $\langle p_3 q_3, 3\rangle$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above. Assume $p_1, p_2, p_3, q_1, q_2, q_3$ are all distinct and are valid primes for RSA to be carried out.

(c) Let's say the secret x was not changed ($e = 3$), so they used the same public keys as before, but did not transmit different messages. How can Eve figure out x?