RSA Cryptosystem

DR. ODELU VANGA

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRI CITY

CHITTOOR, INDIA

RSA cryptosystem

First published:

- Scientific American, Aug. 1977 (Patent up to Sept 21, 2000)

Currently the "work horse" of Internet security:

- Most Public Key Infrastructure (PKI) products.
- SSL/TLS: Certificates and key-exchange.
- Secure e-mail: PGP, Outlook, …

Transport Layer Security
Secure Sockets Layer

RSA trapdoor 1-to-1 function

Parameters: N=pq. N ≈1024 bits. p,q ≈512 bits.
e – encryption exponent. gcd(e, φ(N)) = 1 .

1-to-1 function: **RSA(M) = M^e** (mod N) where $M \in Z_N^*$

Trapdoor: **d** – decryption exponent.
Where $e \cdot \mathbf{d} = 1 \pmod{\varphi(N)}$

Inversion: $RSA(M)^d = M^{ed} = M^{k\varphi(N)+1} = \mathbf{M} \pmod{N}$

$e \cdot d = 1 \bmod \phi(N)$
$ed = k\phi(N)+1$ mod φ(N)
$a^{\phi(m)} = 1 \bmod m$

(n,e,t,ε)-RSA Assumption: For any t-time algorithm A:

$$\Pr\left[A(N,e,x) = x^{1/e}\ (N) :\ \begin{array}{l} p,q \xleftarrow{R} \text{n-bit primes}, \\ N \leftarrow pq,\quad x \xleftarrow{R} Z_N^* \end{array}\right] < \varepsilon$$

Example 1 - Key Setup

$e^{-1} \bmod \phi(N)$

$7^{-1} \bmod 160$

=

1. Select primes: p=17 & q=11
2. Calculate $N = pq$ =17 x 11=187
3. Calculate $\varnothing(N) = (p-1)(q-1)$=16x10=160
4. Select e: gcd(e,160)=1; choose e=7
5. ? Determine d: $\boxed{de=1 \bmod 160}$ and $d < 160$
6. Value is d=23 since 23x7=161= 10x160+1
7. Publish public key PU={7,187} = {e, N}
8. Keep secret private key PR={23,187} = {d, N}

Example - RSA En/Decryption

1. Publish public key
   PU={7,187}
2. Keep secret private key
   PR={23,187}

- RSA encryption/decryption is:
- Given message M = 88
- Encryption:

  $C = 88^7 \bmod 187 = 11$

- Decryption:

  $M = 11^{23} \bmod 187 = \underline{88}$

$C = M^e \bmod N$

$M = C^d \bmod N$

$M = (88^7)^{23} = (88)^{7\times 23} \bmod 187$

$= 88^{7\times 23 \bmod 160} \bmod 187$

$= 88 \bmod 187.$

Example 2

$p = 11$, $q = 7$, $N = 77$, $\Phi(N) = 60$

$e = 37$ ($ed = 481$; $ed \bmod 60 = 1$)

What is d ?

$d = 13$

Let $M = 15$.

Then $C \equiv M^e \bmod N$

- $C \equiv 15^{37} \pmod{77} = 71$

encryption.

$c = m^e \bmod N$

$= 15^{37} \bmod 77$

$= 71$

$M \equiv C^d \bmod n$

- $M \equiv 71^{13} \pmod{77} = 15$

Example 3

$(e, \phi(N)) = 1.$

Parameters:

- $p = 3$, $q = 5$, $N = pq = 15$
- $\Phi(N) =$? 8

$\phi(N) = (p-1)(q-1)$
$= 2 \times 4 = 8$

$d = 3$, $ed = 3 \times 3 \bmod 8$
$= 1.$

Let e = 3, what is d?

Given M=2, what is C?

$c = M^e = 2^3 = 8 \bmod 15$
$= 8$

How to decrypt?

$M = C^d = 8^3 = 2 \bmod 15$

Example

$A \xrightarrow{m^e} B\{n, d\}$

$\{n, e\} = \{187, 7\}$ public

Suppose Alice wishes to send a plaintext message M to Bob using the RSA algorithm.

Bob's public-key is (n, e) = (187; 7). Note that 187 = 17 * 11.

Alice uses an alphabet set of only 10 letters and encode them as

A = 0; C = 1; D = 2; E = 3; I = 4; N = 5; O = 6; R = 7; T = 8; U = 9.

Alice transmits the message in blocks. Each block corresponding to two letters which are encoded into their numerical equivalent, e.g., NO encodes as [56] and then it is encrypted using RSA.

If Alice wants to send the text "NO", what ciphertext will be received by Bob ?

78 = RT

Q: Suppose Bob receives [11], then what was the message transmitted by Alice?

Ans: [88]

e, $(e, \phi(n)) = 1$

$de = 1 \bmod \phi(n)$

$n = p \times q$

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

$\rightarrow \{n, e\}$ - public

$\{n, d\}$ - private

$c = m^e \bmod n$

$m = c^d \bmod n$

Q: $\phi(n)$ - secret | ~~public~~ ??

we can find $d = e^{-1} \bmod \phi(n)$??

Φ(N) implies factorization

Knowing both n and Φ(N), one knows

$N = pq$

$\Phi(N) = (p-1)(q-1) = pq - p - q + 1$

$= N - p - N/p + 1$

$p\Phi(N) = Np - p^2 - N + p$

$p^2 - Np + \Phi(N)p - p + N = 0$

$p^2 - (N - \Phi(N) + 1)\, p + N = 0$

There are two solutions of p in the above equation.

Both p and q are solutions.

Thank You