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, ...

RSA trapdoor 1-to-1 function

Parameters:

N=pq. N \approx 1024 bits. p,q \approx 512 bits.

e – encryption exponent. $gcd(e, \phi(N)) = 1$.

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

Trapdoor:

d – decryption exponent.

Where $e \cdot d = 1 \pmod{\phi(N)}$

Inversion:

$$\mathbf{RSA(M)}^{\mathbf{d}} = \mathbf{M}^{\mathrm{ed}} = \mathbf{M}^{\mathrm{k}\phi(N)+1} = \mathbf{M} \pmod{N}$$

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

$$Pr[A(N,e,x) = x^{1/e}(N):$$

$$\Pr[A(N,e,x) = x^{1/e}(N): \quad p,q^R \leftarrow \text{ n-bit primes,} \\ N \leftarrow pq, \quad x \leftarrow^R Z_N^* \end{bmatrix} < \epsilon$$

Example 1 - Key Setup

- 1. Select primes: p=17 & q=11
- 2. Calculate $N = pq = 17 \times 11 = 187$
- 3. Calculate $\emptyset(N) = (p-1)(q-1) = 16 \times 10 = 160$

e root porto

- 4. Select e: gcd(e, 160) = 1; choose e=7
- 5. ? Determine d: $de=1 \mod 160$ 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 $PR = \{23, 187\} = \{4, N\}$

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:

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

> Decryption:

$$M = 11^{23} \mod 187 = 88$$

e model strong of the strong o

Example 2

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

$$e = 37 \text{ (ed} = 481; ed mod 60 = 1)$$

What is d?

$$d = 13$$

Then $C \equiv M^e \mod N$ • $C \equiv 15^{37} \pmod{77} = 71$

 $M \equiv C^d \mod n$

• $M \equiv 71^{13} \pmod{77} = 15$

Example 3

Parameters:

$$\circ \Phi(N) = ?$$

Let e = 3, what is d?

Given M=2, what is C?

How to decrypt?

$$(e)$$

$$\phi(N) = (p-1)(z-1)$$

$$= 2 \times 4 = 8$$

$$= 2 \times 4 = 8$$

$$d?$$

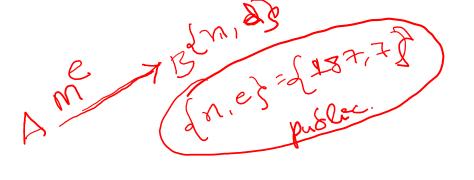
$$d = 3 + ed = 3 \times 3 \text{ mod } 8$$

$$c = M^{2} = 2^{3} = 8 \text{ mod } 3$$

$$c = M^{2} = 2^{3} = 8 \text{ mod } 3$$

$$m = C = 8^{3} = 2 \text{ mod } 3$$





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?

9: Suppose Bod receives [11], has what. was the malsage transmitted by Alice? Ans: [88] $e, (e, p(n)) = n = p \times 2$ e, (e, p(n)) = (p - 1)(z - 1) f(n, e) = p(x) d(n) = (p - 1)(z - 1) $C = m \mod n$ $n = p \times 2$ $C = m \mod n$ m = cd mod n g: $\phi(n) - suid | pullec 9.7.$ we can find d= et mal p(N) 15

$\Phi(N)$ implies factorization

Knowing both n and $\Phi(N)$, 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