RSA Algorithm

- Proposed by Rivest, Shamir, and Adleman in 1977.
- Best known & widely used public-key scheme
- Based on exponentiation in a finite (Galois) field over integers modulo a prime.
- Security due to the cost of factoring large numbers.
- Public-key algorithms rely on two keys where:
- it is computationally infeasible to find decryption key knowing only the algorithm & encryption key
- it is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known
- either of the two related keys can be used for encryption, with the other used for decryption (for some algorithms)

The RSA scheme is a cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 21024.

For this example, the keys were generated as follows.
1. Select two prime numbers, p = 17 and q = 11.
2. Calculate n = pq = 17 * 11 = 187.
3. Calculate f(n) = (p - 1)(q - 1) = 16 * 10 = 160.
4. Select e such that e is relatively prime to f(n) = 160 and less than f(n); we choose e = 7.
5. Determine d such that de K 1 (mod 160) and d 6 160. The correct value is
d = 23, because 23 * 7 = 161 = (1 * 160) + 1; d can be calculated using the extended Euclid's algorithm.
The resulting keys are public key PU = {7, 187} and private key PR = {23, 187}.
The example shows the use of these keys for a plaintext input of M = 88.
For encryption, we need to calculate C = 887 mod 187. Exploiting the properties of modular arithmetic, we can do this as follows.
887 mod 187 = [(884 mod 187) * (882 mod 187)
* (881 mod 187)] mod 187

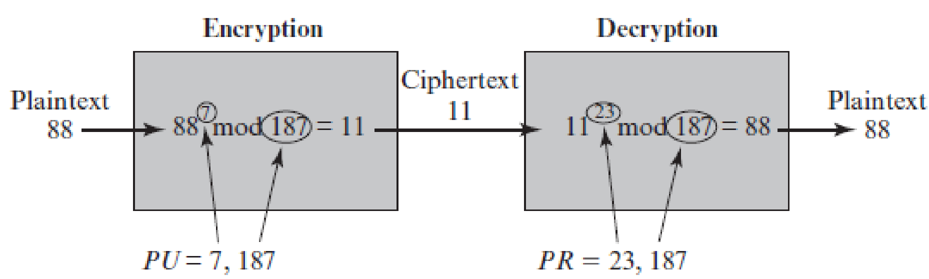
881 mod 187 = 88
882 mod 187 = 7744 mod 187 = 77
884 mod 187 = 59,969,536 mod 187 = 132
887 mod 187 = (88 * 77 * 132) mod 187 = 894,432 mod 187 = 11
For decryption, we calculate M = 1123 mod 187:
1123 mod 187 = [(111 mod 187) * (112 mod 187) * (114 mod 187) * (118 mod 187) * (118 mod 187)] mod 187
111 mod 187 = 11
112 mod 187 = 121
114 mod 187 = 14,641 mod 187 = 55
118 mod 187 = 214,358,881 mod 187 = 33
1123 mod 187 = (11 * 121 * 55 * 33 * 33) mod 187
= 79,720,245 mod 187 = 88

Key Generation by Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

The RSA Algorithm



Example of RSA Algorithm

RSA En/decryption

to encrypt a message M the sender:
obtains public key of recipient PU={e,n}
computes: C = Me mod n, where 0≤M<n
to decrypt the ciphertext C the owner:
uses their private key PR={d,n}

computes: M = Cd mod n
note that the message M must be smaller than the modulus n (block if needed)

RSA Key Setup

each user generates a public/private key pair by:
selecting two large primes at random: p, q
computing their system modulus n=p.q
note ø(n)=(p-1)(q-1)
selecting at random the encryption key e
where 1<e<ø(n), gcd(e,ø(n))=1
solve following equation to find decryption key d
e.d=1 mod ø(n) and 0≤d≤n
publish their public encryption key: PU={e,n}
keep secret private decryption key: PR={d,n}

Because of Euler's Theorem:
$a^{ø(n)}$ **mod n = 1 where gcd(a,n)=1**

in RSA have:
n=p.q
ø(n)=(p-1)(q-1)
carefully chose e & d to be inverses mod ø(n)
hence e.d=1+k.ø(n) for some k
hence :

Cd = Me.d = M1+k.ø(n) = M1.(Mø(n))k
= M1.(1)k = M1 = M mod n

Steps of the RSA Algorithm

1) Each user generates a public/private key pair by:

- Selecting two large primes at random - p, q.
- Computing their system modulus N=p.q.
- ø(N) = (p-1) (q-1).

2) Selecting at random the encryption key (e):
- $1 < e < ø(N)$, $\gcd(e, ø(N)) = 1$.

3) Find decryption key (d):
- $e \cdot d = 1 \bmod ø(N)$ and $0 \le d \le N$.

4) Publish their public encryption key: KU = {e ,N }.

5) keep secret private decryption key: KR = { d, p, q }.

6) To encrypt a message M the sender:
- Obtains public key of recipient KU={e,N}
- Computes: $C=M^e \bmod N$, where $0 \le M < N$

7) To decrypt the ciphertext C the owner:
- Uses their private key KR={d,p,q}
- Computes: $M=C^d \bmod N$

RSA Examples:

C= cipher text

P= m =plain text

E= public key

N =product of two prime Multiplication

D= private key

$d=e^{-1} \bmod ø(n)$

$e=d^{-1} \bmod ø(n)$

$e*d \bmod ø(n) =1$

$ø(n) = (p-1)(q-1)$

$c=m^e \bmod n$ for encryption

$m=c^d \bmod n$ for decryption

Ex1: Let p=11, q=13, e=11, m= systems =7 find the private key d

Sul:

n=p*q

n=11*13

n=143

ø(n) = (p-1) (q-1)

ø(n)=10 *12

ø(n)=120

e*d mod ø(n)=1

11* d mod 120=1

11* 11 mod 120=1

d=11

c=m^e mod n **for encryption**

c= m^e mod 143

c= 7^{11} mod 143

c= 1977326743 mod 143

c=106

m=c^d mod n **for decryption**

m= 106^{11} mod 143

m=7

Ex2: Find keys d and p for the RSA Cryptos system were

P=7, q=11

Sul:

P=7, q=11

n=p*q

n= 7*11

ø(n) = (p-1) (q-1)

ø(n) = 6*10

ø(n) = 60

e*d mod ø(n) = 1

Let

e*d=x

X mod ø(n) = 1

X mod 60 = 1

121 mod 60 = 1

11 *11 mod 60 = 1

X= 11 *11

Where x=e*d Therefor

e=11, d=11

Homework

Ex/ p=3,q=11,e=7,m=2 encrypt and decrypt using RSA Algorithm?

Inverse

$X= a^{p-2}$ mod p   **P must be Prime**

15^{-1} mod 17 =8   **17 must be Prime**

15^{17-2} mod 17

15^{15} mod 17

$15^{5} * 15^{5} * 15^{5}$ mod 17

15^{5}= 759375 mod 17 =2

2 * 2 * 2=8

Sul2:

15^{-1} mod 17 =8

17+17=34+1 / 15=2.3

34+17=51+1 / 15=3.4

51+17=68+1 / 15=4.6

68+17=85+1 / 15= 5.7

85+17=102+1 / 15=6.86

102+17=119+1 / 15= 8