RSA

CHITRANG SRIVASTAVA

Introduction to RSA

- Choose *two* distinct *prime* numbers *p* & *q*.
- Compute n = p .q , key length
- $\boldsymbol{\varphi(n) = (p - 1)(q - 1)}$
- $\boldsymbol{1 < e < \varphi(n)}$ **&** $\boldsymbol{\gcd(e, \varphi(n)) = 1}$
- $\boldsymbol{d \cdot e \equiv 1 \pmod{\varphi(n)}}$
- public = (**n**, **e**) Encrypt = $\boldsymbol{m}^{e}$ mod n = C
- private = (**n**, **d**) Decrypt = $\mathbf{C}^{d}$ mod n
- Public: (**23**, **143**) M=5 ->5^{23} mod 143 = 125
- Private:(**47**, **143**) 125^{47} mod 143 = 5

Euler Totient Function φ (phi)

- **Counts** number that are **relative prime** to it.
- Example n =9 *φ(9)* = 6
- 9 = 3^2 (Fundamental Theorem)
- $\varphi(9) = 9 \cdot (1 - 1/3) = 6$
- For any prime *φ(p) = p-1*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

1	9	Y
2	9	Y
3	9	N
4	9	Y
5	9	Y
6	9	N
7	9	Y
8	9	Y

FAQ

Why e coprime to $\varphi(n)$

Let us take the example you give: ***N=65*** and ***e=3***.

Then, if we encrypt the plaintext **2**, we get $\mathbf{2^3 \bmod 65=8}$.

However, if we encrypt the plaintext **57**, we get $\mathbf{57^3 \bmod 65=8}$
Hence, if we get the cipher text **8**, we have no way of determining whether that corresponds to the plaintext 2 or 8.

Making sure e and $\phi(N)$ are relatively prime ensures this doesn't happen.

How to generate p, q in RSA?

Why use congruence in RSA equation

$0 \equiv 2 \pmod 2$ but $(0 \bmod 2) \neq 2$

Fermat's Theorem

- $a^{p-1} \equiv 1 \bmod p$, **p** is prime number.
- Primality testing, Randomized Algorithm.
- Quiz: $2^{100001} \bmod 11$?

Euler Theorem

- $a^{\varphi(n)} \equiv 1 \pmod{\mathbf{n}}$ n can be composite
- RSA depend on it.
- $e.\,d \equiv 1 \bmod \varphi(n) \Rightarrow k\cdot\varphi(n) = e.d - 1$
- $C = M^e \bmod n \Rightarrow C^d \equiv M^{ed} \bmod n \Rightarrow M^{k\varphi(n)+1}$
- $M \cdot M^{k\varphi(n)} \pmod{n} = M$
- Quiz : $2^{245} \bmod 35$?

Congruence (≡)

a & ***b*** are said congruent **modulo n** , when a and b have same remainder when divided by n.

$$\mathbf{a \equiv b \pmod{n}}$$

Example a= 37 , b = 57 n =10
$37 \equiv 57 \pmod{10}$

Alternatively, a-b is divisible by n

"x = y mod n" means x is equal to the remainder on dividing y by n
"$x \equiv y \pmod{n}$" means x and y have the same remainder when divided by n. In the latter case x has an infinite range of possible values of the form x = y + kn. We are usually interested in the unique value of x in the range $0 \le x < n$ anyway, so we might be a bit sloppy in their use.

If we add four hours to 11 o'clock, if we work with 12-hours, we do not get 11+4=15, we instead call this 3 o'clock. Similarly if the time is 2 and we ask what was the time 3 hours ago, we do not respond, "It was -1", we call this 11 o'clock.

Euclidean Algorithm

Suppose you have to find **GCD** of two number(**26, 11**)

26 = **11***2 + **4**
11 = **4*** 2 +**3**
4 = **3*** 1 +**1**
3 = **1***3 + **0**

11 ⎡26 **2**
22
4 ⎡11 **2**
8
3 ⎡4 **1**
3
1 ⎡3 **3**
3
0

GCD (26, 11) = 1

Extended Euclidean Algorithm

- Idea is to represent the GCD in the linear form of the input.
  For example
  1 = 26 * x + 11 * y [where x and y are Integers]
  We can traverse backward from equation # 6
- 1 = 4 - (3 * 1)
- 1 = 4 - (11 -4*2) => 4*3 - 11
- 1 = (4*3 – 11) => (26 -11*2)*3 - 11
- 1 = **26*3 - 11*7** ∴x = 3 , y =-7
- Hence GCD is represented in some linear form of inputs.

Modular Multiplicative Inverse

- d . e ≡ 1 mod n
- If **n is not prime** we can use **Extended Euclidean Algorithm** to find inverse. If n is prime we can use Fermat's Little Theorem.
  Example
  11 .e = 1 mod 26
  Since 26 is not prime we will use Extended Euclidean Algorithm to represent their GCD(11, 26) in some linear form
- **1** ≡ **26 *3 – 11*7**
- 1 mod 26 ≡ **-7 * 11** ∴x = -7 or 19 since -7 **≡** 19 mod 26

Integer Factorization Problem

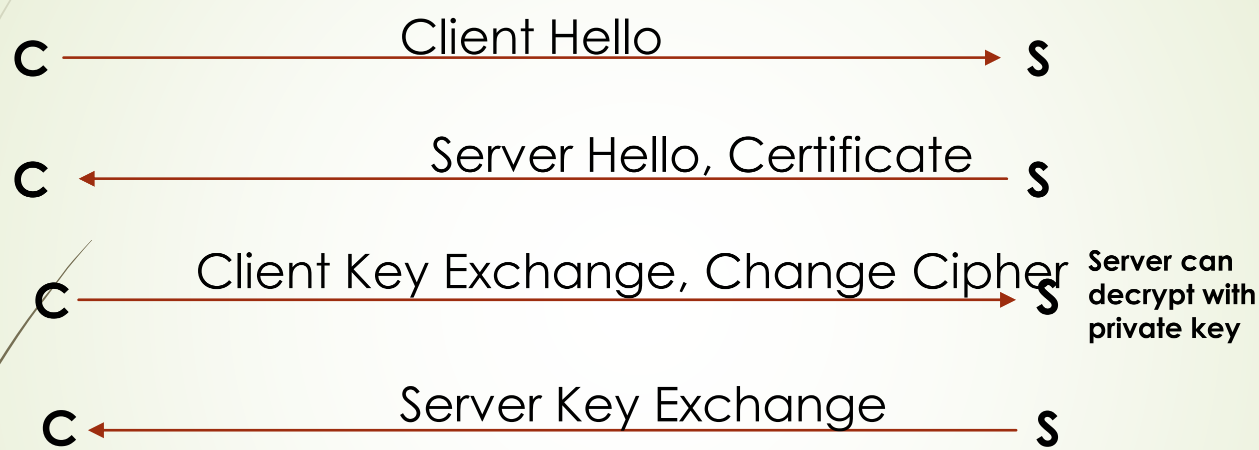
$\boldsymbol{d \cdot e \equiv 1 \pmod{\varphi(n)}}$

e & ***n*** are known but in order to solve above equation one has to find $\varphi(n)$ and for that one has to factor ***n***.

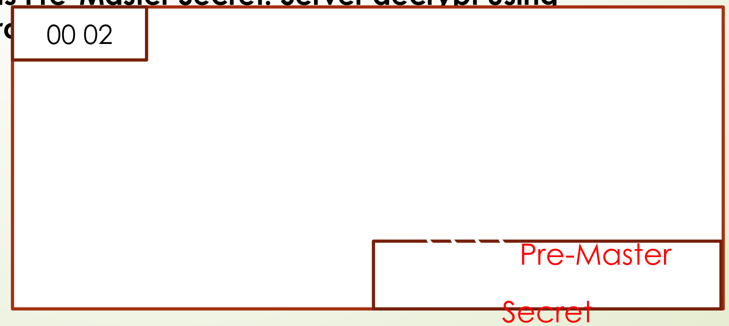
Largest prime yet factored was RSA-768, a 768-bit number with 232 decimal digits

Pollard-Rho, Quadratic Sieve, GNFS.

RSA in TLS 1.2



Generates a 48 byte random number and encrypt with public key of Server certificate & sent in PKCS#1v1.5 format. This random number knows as Pre-Master Secret. Server decrypt using private key and then both side proceed to genera



Public Key in Certificate

- Export certificate from browser
- Extract public key from certificate **`openssl x509 -pubkey -noout -in cert.pem > pubkey.pem`**

```
openssl rsa -pubin -inform PEM -text -noout < pubkey.pem

Public-Key: (2048 bit)

Modulus:

    00:cf:15:ab:42:43:17:b3:39:7c:25:ea:ce:b2:d6:

    ad:b5:a0:4e:2f:47:44:0d:d9:c4:09:ca:e0:54:9d:

    15:6c:b4:d9:3b:00:63:e9:e4:32:12:69:e8:ed:3a:

    8c:62:e4:7f:c9:1f:8f:55:fc:b5:eb:d9:4a:59:e9:

    ad:11:07:a6:0b:c0:ec:25:de:1d:df:5c:c8:13:a8:

    08:ed:22:15:af:b4:44:4c:07:43:c4:3c:ee:8f:ff:

    3b:ee:02:89:96:84:9d:2b:28:0f:20:ae:f1:e4:c8:

    33:4f:ca:49:31:d9:31:22:16:8c:3c:3f:90:2a:4b:

    12:1b:74:91:db:71:b0:94:6e:e7:ea:90:44:14:3f:

    79:37:a8:a0:db:a9:50:a7:ab:7a:9a:c9:fb:f0:cb:

    43:c4:7d:9e:d8:8a:ef:54:dd:c2:78:23:5b:6d:c8:

    b9:0e:00:c8:67:ee:96:21:c8:c2:95:4c:b6:97:b1:

    8b:b1:64:7b:50:cb:53:40:2f:32:3e:52:f0:89:c0:

    e7:28:7f:65:33:b8:9e:15:0b:4d:ec:eb:4c:b7:1d:

    aa:d5:40:1d:55:0c:99:c8:06:ab:b9:7c:49:de:81:

    12:e3:96:72:1b:76:fb:a3:4d:e7:28:7d:c0:b0:b6:

    42:bf:ae:63:4e:33:96:26:1c:a9:cb:54:84:6d:b0:

    d0:77

Exponent: 65537 (0x10001)
```

Private Key

```
RSAPrivateKey ::= SEQUENCE {
  version           Version,
  modulus           INTEGER,  -- n
  publicExponent    INTEGER,  -- e
  privateExponent   INTEGER,  -- d
  prime1            INTEGER,  -- p
  prime2            INTEGER,  -- q
  exponent1         INTEGER,  -- d mod (p-1)
  exponent2         INTEGER,  -- d mod (q-1)
  coefficient       INTEGER,  -- (inverse of q) mod p
  otherPrimeInfos   OtherPrimeInfos OPTIONAL
}
```

$d \cdot e \equiv 1 \pmod{\varphi(n)}$ can be solved using above information.

Garner's Formula: https://www.di-mgt.com.au/crt_rsa.html

Mersenne Prime

- $M_p = 2^p - 1$.
- $M_5 = 2^5 - 1 = 31$
- Largest known prime number is Mersenne prime. $M_{82,589,933}$
- Only 51 of them
- We want to compute 632 mod 31
- 632 in binary is 100111100, we split the number in groups of 5 bits (because we are using M5): 10011 and 11000, now we add those parts:
- 10011 + 11000 = 101011 since the result is longer than 5 bits we repeat:
- 010011 + 1 = 1100
- And 1100 is 12 so 632 mod 31 is 12
- Notice we have computed a modulo operation just doing additions!
- https://www.mersenne.org/

Homomorphic Encryption

Alice: private (**47, 143**)
Public: (**23, 143**)

Alice wants to compute area of rectangle **w=7, h=3**
But don't know formula.
She can take help of Bob but don't want to reveal input.

Alice encrypt input and send to Bob.
$C_w = 7^{23} \mod 143 = 2$
$C_y = 3^{23} \mod 143 = 126$

Bob return 2 *126 =252

$252^{47} \mod 143 =$ **21**

- Homomorphic property of RSA is **multiplication**.
- Many other crypto system provide other property like addition/XOR etc.
- **Fully Homomorphic encryption** can do any kind of operation on encrypted inputs.

http://homomorphicencryption.org/introduction/

Attacks on RSA

- Common Modulus: If **N** is factor for one entity, it can also be used for other entity if they are also using same **N**.
- When e & m are small
- CopperSmith Attack: If a message is sent to more recipient which has same **e** but different **n**, Chinese Remainder Theorem can be used.
- Plain RSA is not **semantically secure.** Attacker can launch CPA and test if they are equal to cipher text.
- CCA: RSA is malleable cipher. OEAP used to provide randomness.
- Bleichenbacher Attack & ROBOT.
- http://crypto.stanford.edu/~dabo/pubs/abstracts/RSAattack-survey.html

Quiz

1. Compute GCD(1701, 3768)

2. Is **6666663 ≡ 77892839283 mod 10** ?

3. In RSA, Φ(n) = _______ in terms of p and q.
   a) (p)/(q)
   b) (p)(q)
   c) (p-1)(q-1)
   d) (p+1)(q+1)

4. For p = 11 and q = 19 and choose e=17. Apply RSA algorithm where message=5 and find the cipher text.
   a) C=80
   b) C=92
   c) C=56
   d) C=23

5. In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 35. Then the private key of A is ____________.

   (A) 11

   (B) 13

   (C) 16

   (D) 17