have to study Again

Discrete Structures

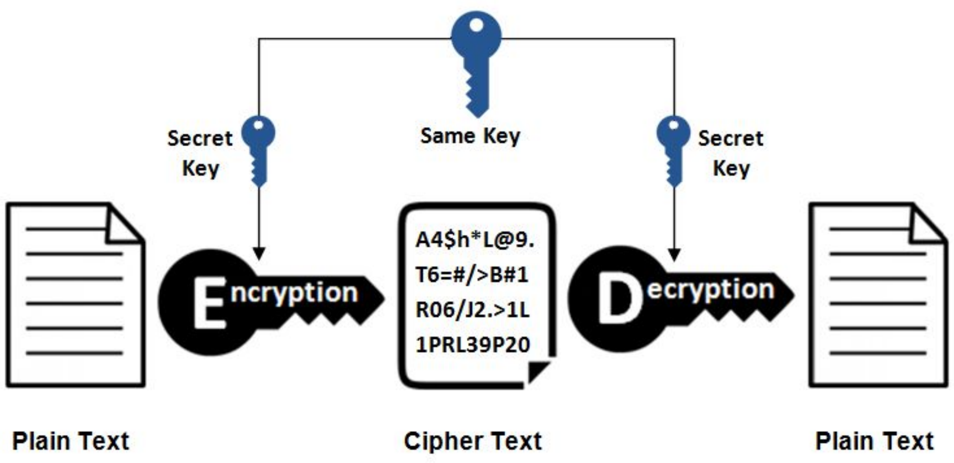
Day 5

Modern day cryptosystem are divided into two:

Symmetric key cryptography:

The sender and receiver uses the same key (private key).

Symmetric Encryption

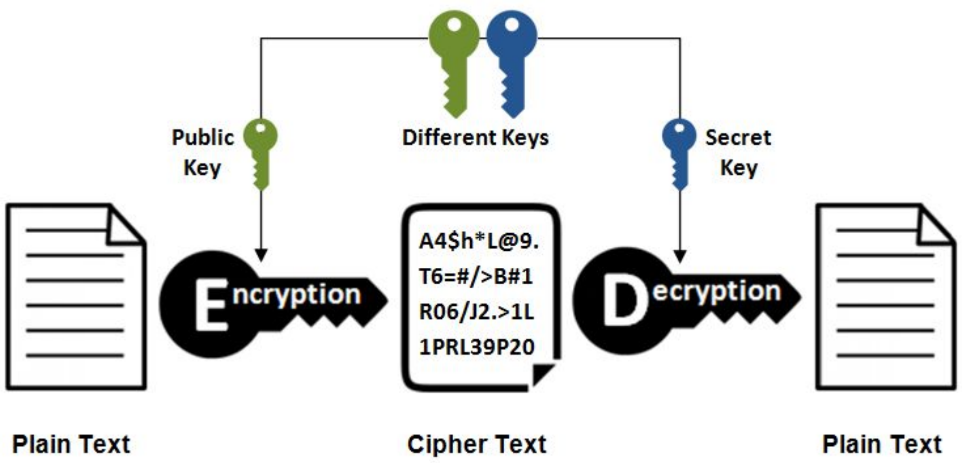


Asymmetric key cryptography:

Two keys for each communicating entity. A private key and a public key. If A and B are the communicating entity.

A's key are (private_A and public_A). Similarly, B's key are (private_B and public_B).

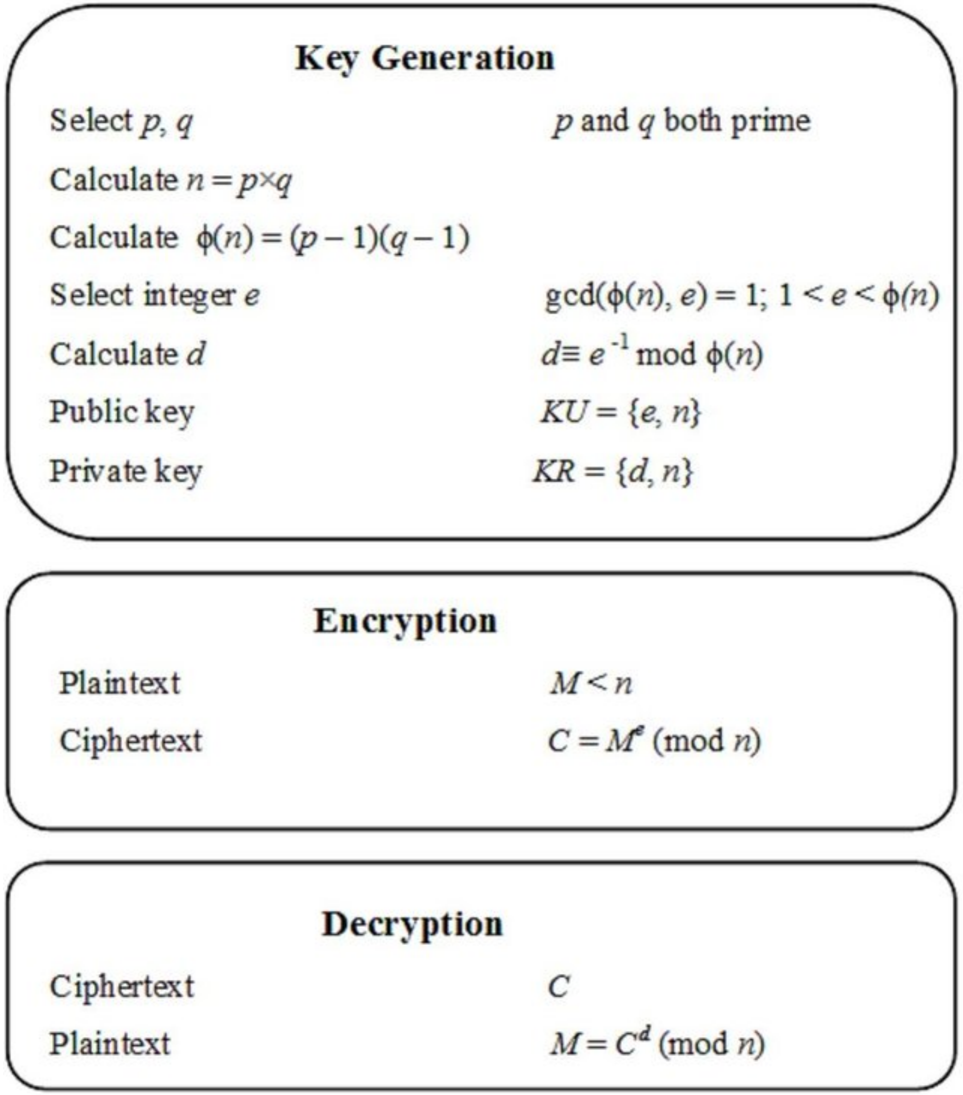
Asymmetric Encryption



RSA (Rivest Shamir Adleman) cryptosystem

RSA is one of the first public-key cryptosystems and is widely used for secure data transmission designed by Rivest, Shamir and Adleman. In such a cryptosystem, the encryption key is public and distinct from the decryption key which is kept secret. RSA depends on the difficulty to factorize the product of two large prime.

Key generation, encryption and decryption algorithm



Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext	$M < n$
Ciphertext	$C = M^e \pmod{n}$

Decryption

Ciphertext	C
Plaintext	$M = C^d \pmod{n}$

- Example
  - Bob chooses 7 and 11 as p and q and calculates n = 7*11=77.
  - The value of $\varphi(n) = (7-1)(11-1) = 60$.
  - Bob choses e=13 and computes d :
  - $d \equiv e^{-1} \mathrm{mod} \varphi(n)$

    i.e. $d \equiv 13^{-1} \mathrm{mod}\ 60$ (apply Extended Euclidean algorithm to find the inverse.

    On computation you will get d=37.

    Bob announces ‘e’ and ‘n’ as public and keeps ‘d’ as secret key.

- Imagine Alice wants to send the plaintext (M) 5 to Bob. She use the public key of Bob to generate the cipher text ‘C’ given by the formula $C = M^e mod\ n$.

So, $C = 5^{13} mod\ 77$

$$\text{Cipher text } C = 26.$$

- Bob on receiving the ciphertext $C = 26$, uses his secret/private key to decipher.
- Plaintext $\mathrm{M} = C^d mod\ n$

$$M = 26^{37} mod\ 77$$

$\mathrm{M} = 5$ (which is the plaintext sent by Alice).

Q. Let p=23, q = 31, Bob Choses e=83. Compute d? If Alice wants to sent the text “CSE”, the ASCII code is (67, 83, 69). Find the cipher text for each ASCII code. Convert back the cipher text to plaintext using the private key ‘d’

- **KEY EXCHANGE**

- Two parties can use to exchange a secret key over an insecure communications channel without having shared any information in the past. Generating a key that two parties can share is important for many applications of cryptography

- For example, for two people to send secure messages to each other using a private key cryptosystem they need to share a common key.

- The **Diffie-Hellman key agreement protocol**, after Whitfield Diffie and Martin Hellman,

-

Diffie-Hellman key agreement protocol

- Suppose that Alice and Bob want to share a common key. The protocol follows these steps, where the computations are done in Z_p.

(1) Alice and Bob agree to use a prime *p* and g primitive root of *p*.

g is a primitive root modulo *p* if for every integer *a* coprime to *p*, there is an integer *k* such that $g^k \equiv a \pmod{p}$

p=5, g=2, a: numbers that are coprime to p (1,2,3,4).

$2^1 \equiv 2\ mod 5$; $2^2 \equiv 4\ mod 5$; $2^3 \equiv 3\ mod 5$; $2^4 \equiv 1\ mod 5$

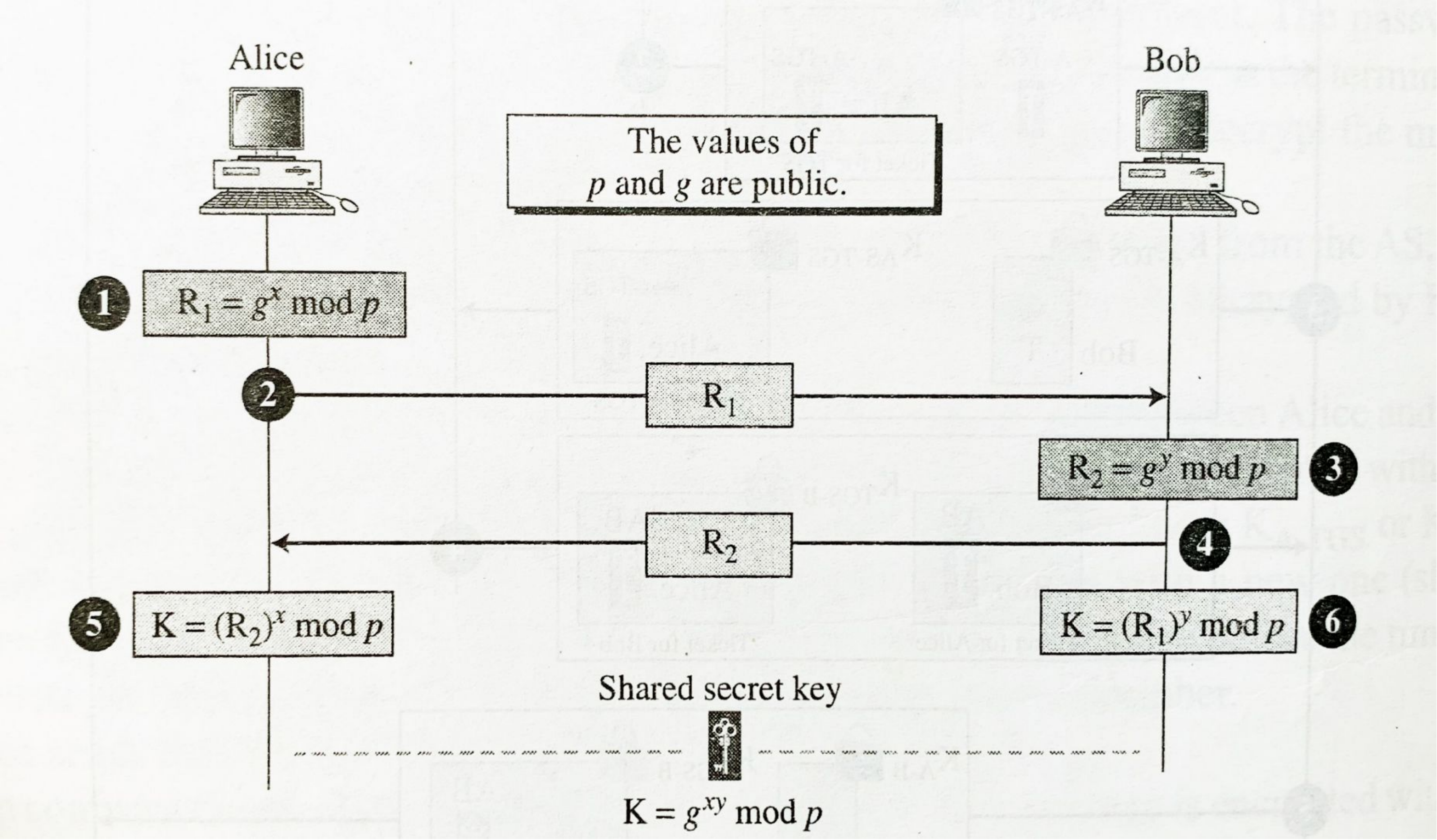
(2) Alice chooses a secret integer x and sends $g^x mod\ p$ to Bob.

(3) Bob chooses a secret integer y and sends $g^y mod\ p$ to Alice.

(4) Alice computes $(g^y)^x mod\ p$.

(5) Bob computes $(g^x)^y mod\ p$.

- At the end of this protocol, Alice and Bob have computed their shared key, namely $(g^y)^x mod\ p = (g^x)^y mod\ p$.



g=7, p = 11, x= 4 , y=5

Girls compute:

R_1:

$R_2^x\ mod\ p$:

Boys compute:

R_2:

$R_1^y\ mod\ p$:

DIGITAL SIGNATURES

- Not only can cryptography be used to secure the confidentiality of a message, but it also can be used so that the recipient of the message knows that it came from the person they think it came from.
- Digital signature can prove the authenticity of the sender of the message.
- A digital signature needs a public-key system. The signer signs with the private key; the verifier verifies with the signer’s public key.

- RSA Digital signature schemes

  - Signing:

    Alice creates a signature out of the message Using her private exponent, $S = M^d mod\ n$ And sends the message and the signature to Bob.

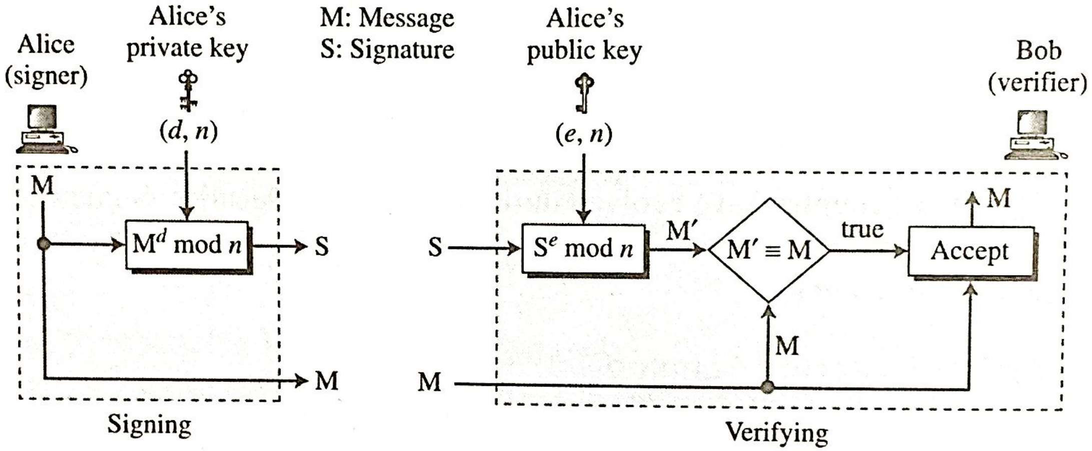


Fig. 2. RSA digital signature scheme

  - Verifying:

    Bob receives M and S. Bob applies Alice's public exponent to signature to create a copy of the message $M' = S^e mod\ n$. Bob compares the value of M' with the value of $M.$ If the two values are congruent, Bob accepts the message.

$$M' \equiv M\ mod\ n$$
$$\rightarrow S^e \equiv M\ mod\ n$$
$$\rightarrow M^{d \times e} \equiv M\ mod\ n$$

** From Euler's theorem $d \times e = 1\ mod\ \varphi(n)$**

- example:
  - Let p and q be 7 and 11. n = 7*11=77.
  - The value of $\varphi(n) = (7-1)(11-1) = 60$.
  - Sender choses e=13 and computes d :
  - $d \equiv e^{-1} \text{mod} \varphi(n) = 37$.

Q. M=8. Find S in the sender side. Verify the message M and the signature received in the receiver side?