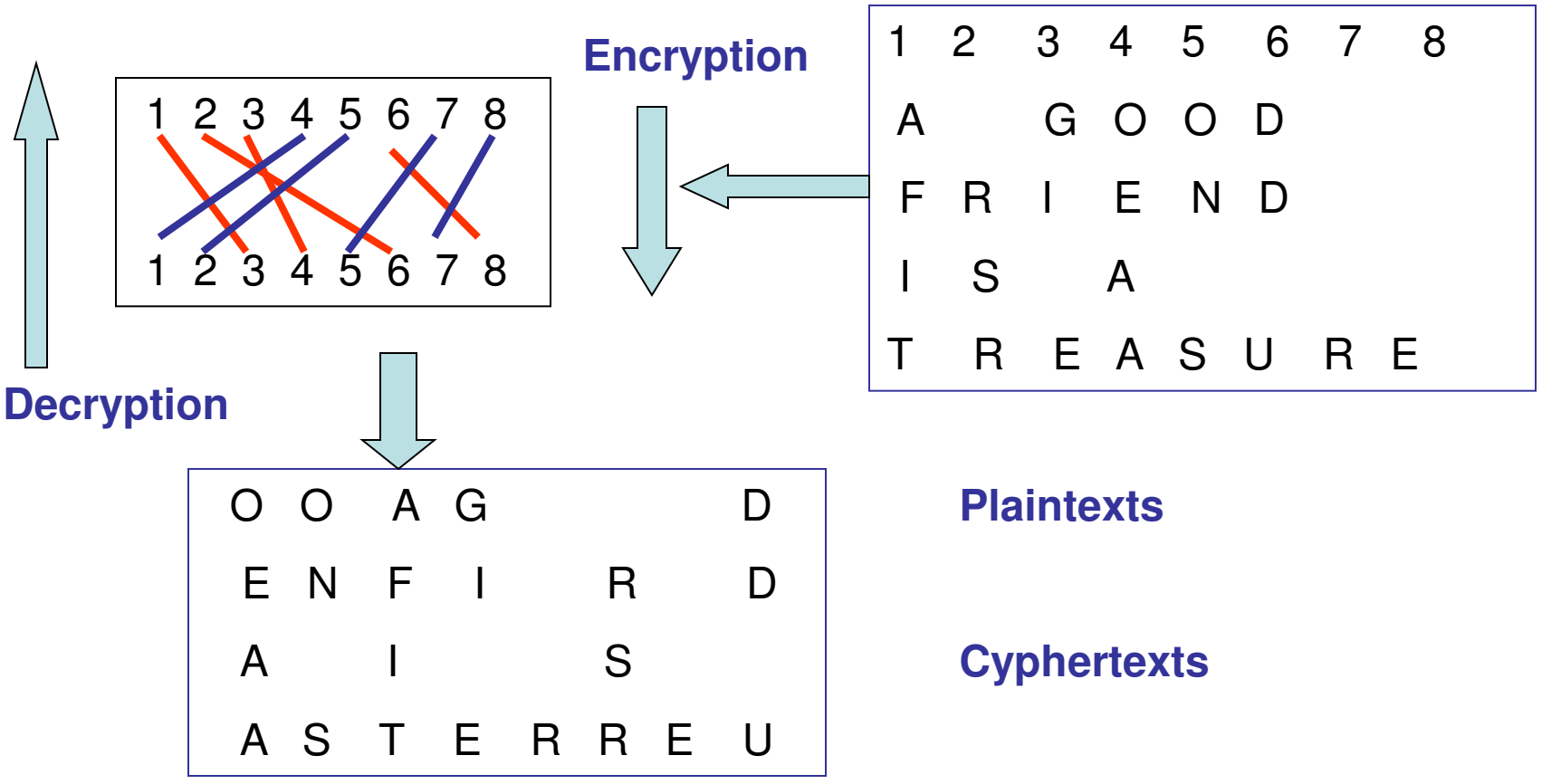
Cryptography (DES+RSA)

by

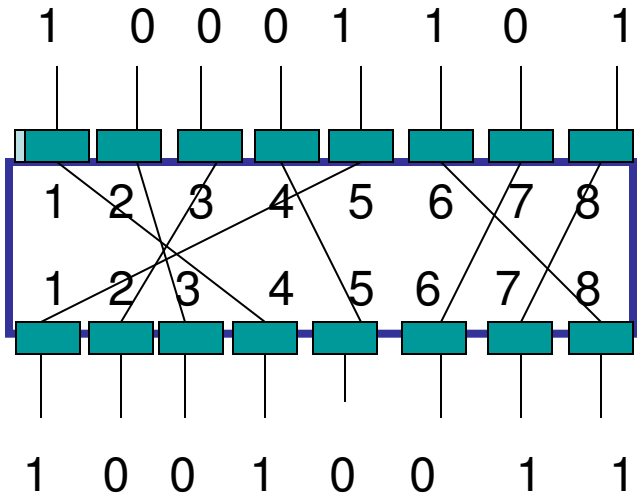
Amit Konar

Dept. of Math and CS, UMSL

Transpositional Ciphers-A Review



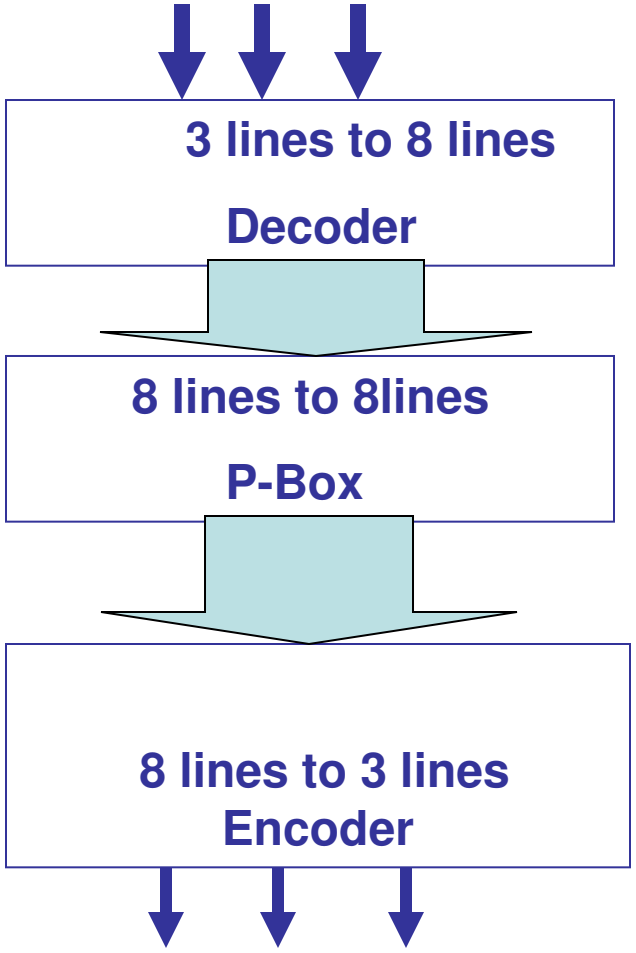
Digital P-box



Enciphering

A **P-box (Permutation box)** performs transposition at the bit level. It can be implemented by hardware or software, but hardwired realization is faster.

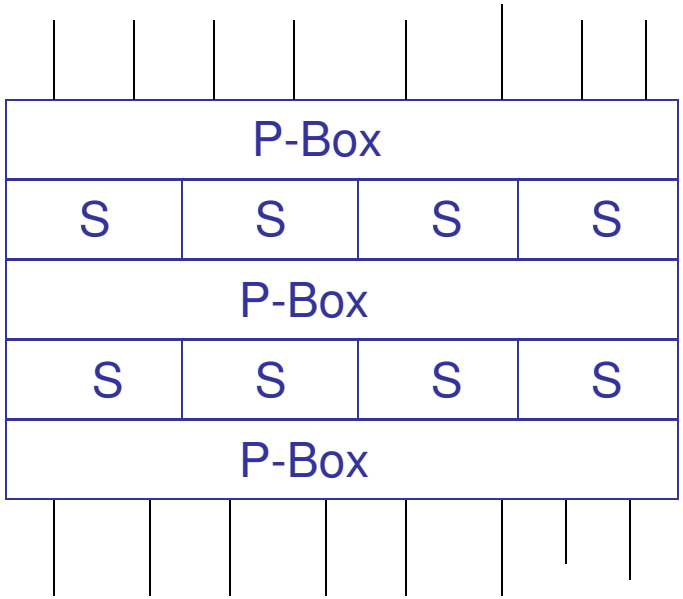
S-Box



An S-box (substitution box) performs substitution at the bit level.

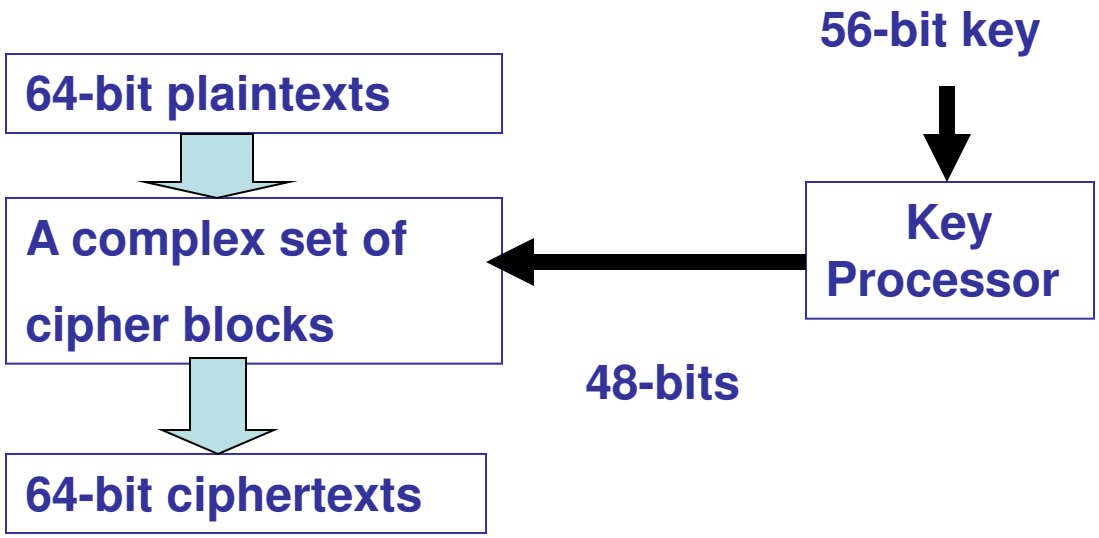
Example: Suppose 2 (010) is the input. Decoder's output is 00000010. P-box's output is 01000000. Encoder output is 6 (110)

Product Block

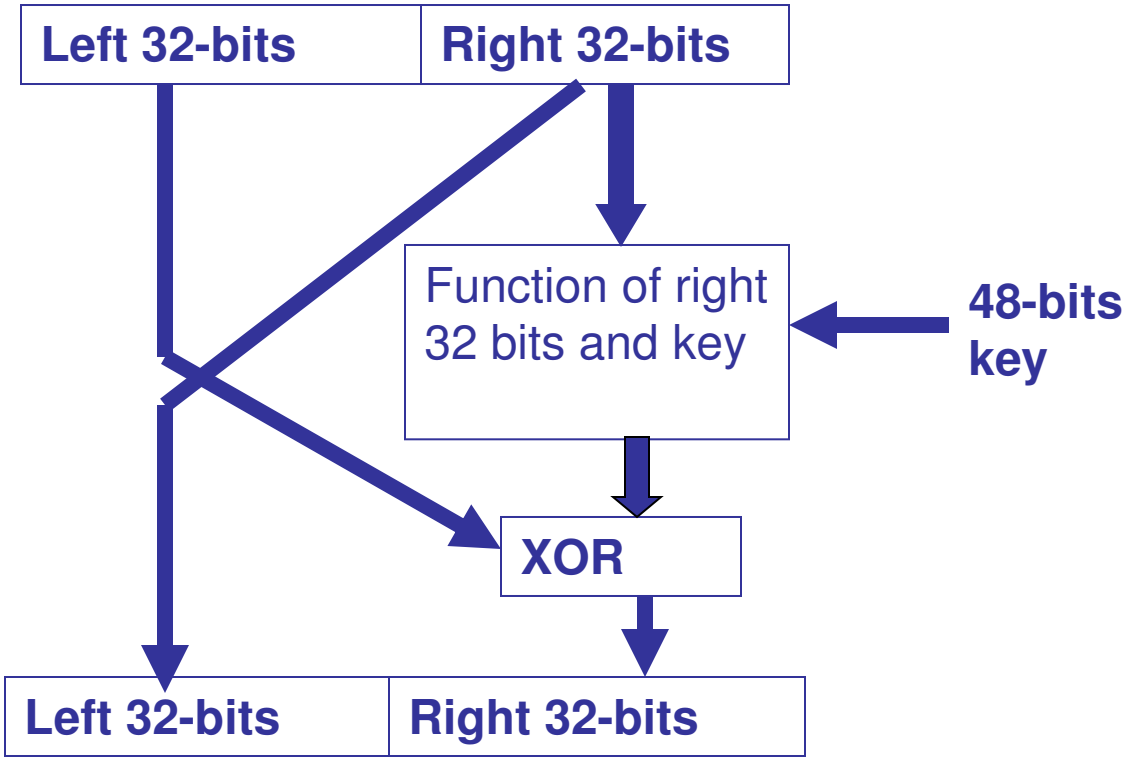


The **P-boxes** and **S-boxes** can be combined to get more complex cipher blocks, called **product blocks**.

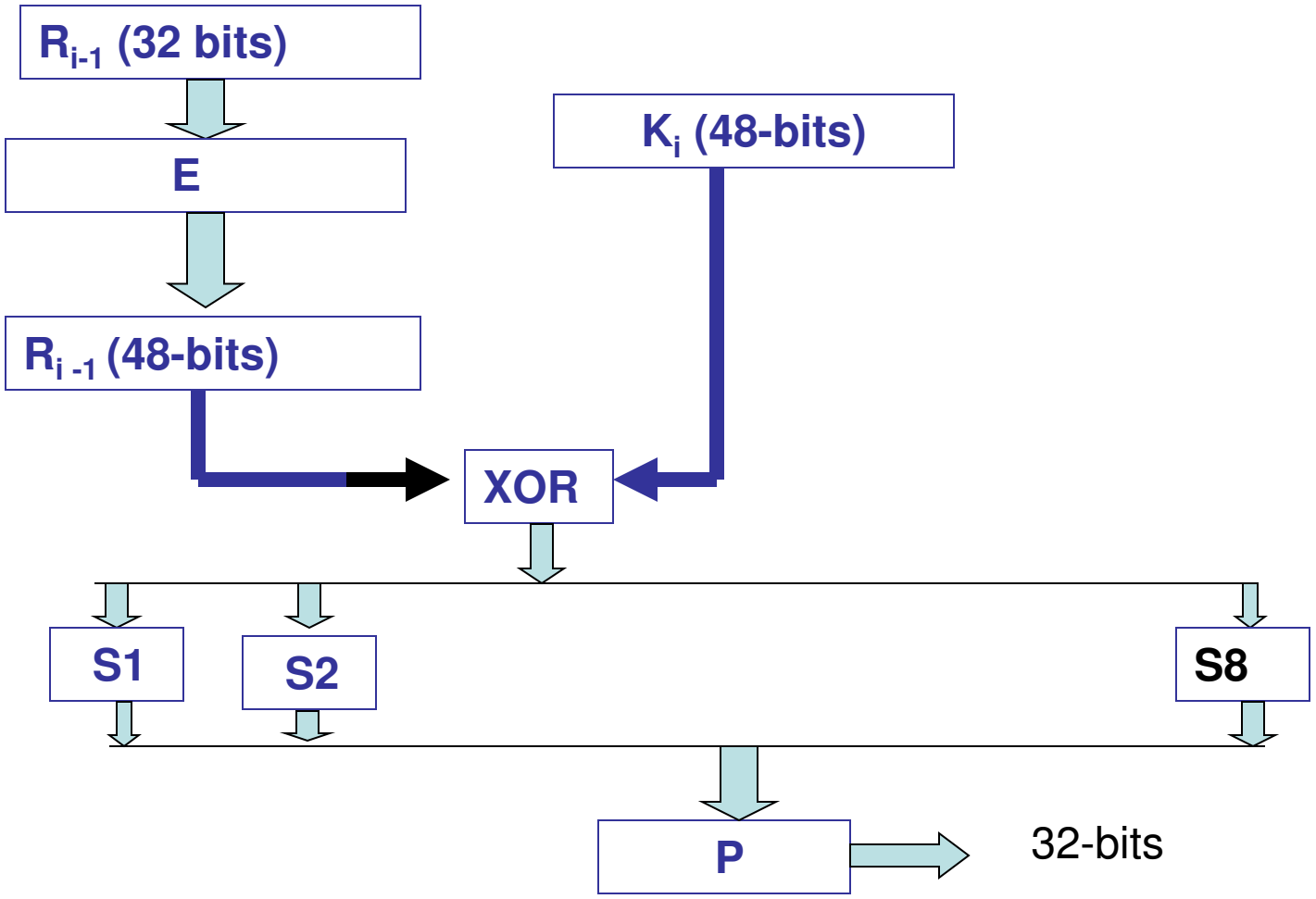
Data Encryption Standard (DES)



Iteration Block



The f-function



Public Key Cryptography

In public key cryptography, we have two keys: one private key and the other public key.

A public Key cryptosystem must meet the following **conditions:**

1. Given the keys, the enciphering and deciphering processes should be simple.
2. Deriving the private key from the public key should be computationally infeasible.
3. Determining the private key from a chosen plaintext attack should be computationally infeasible.

Defining Totients in Public Key Cryptography

Totient: Let p and q be two prime numbers and n = p q. Then the totient $\Phi(n)$ is the number less than n with no factors common with n.

Example: Let p=5 and q=2. So, n=10. Then the numbers that are less than 10 are relatively prime to 10 (i.e. no factors common with 10) are 1, 3, 7 and 9. So, $\Phi(10)=4$. Similarly, when n=21, the nos. that are relatively prime to 21 are 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19 and 20. Therefore, $\Phi(21) =12$.

Defining Keys in Public Key Cryptography

Given n, choose an integer e <n, that is relatively prime to Φ(n). Find a second integer d, such that

e. d mod Φ(n) =1

then **the public key is (e, n),** and

the private key is d.

Encryption and Decryption in Public Key Cryptography

The RSA Method after its inventors (**R**ivest, **S**hamir **and A**dleman)

Let m be a message. Then

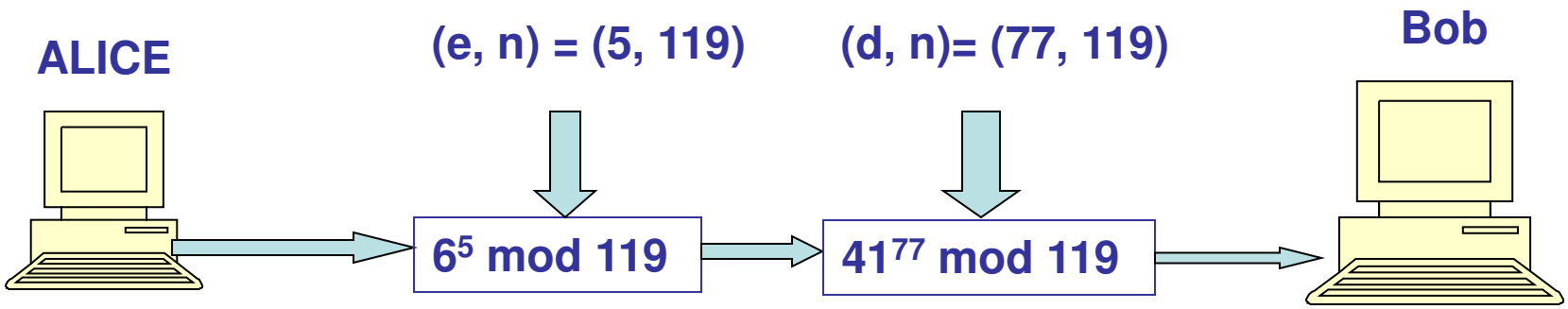
ciphertext c= m^e mod n, and

decrypted plaintext m= c^d mod n

where

public key is (e, n) and private key is d or (d, n), such that e. d mod Φ(n) =1.

Example: The RSA Method



Public key (e, n) = (5, 119)

Private key (d, n)= (77, 119)

Is RSA really Effective?

If an intruder knows the decryption algorithm and n= 119, the only thing missing is d= 77. Why couldn't the intruder use trial and error to find d?

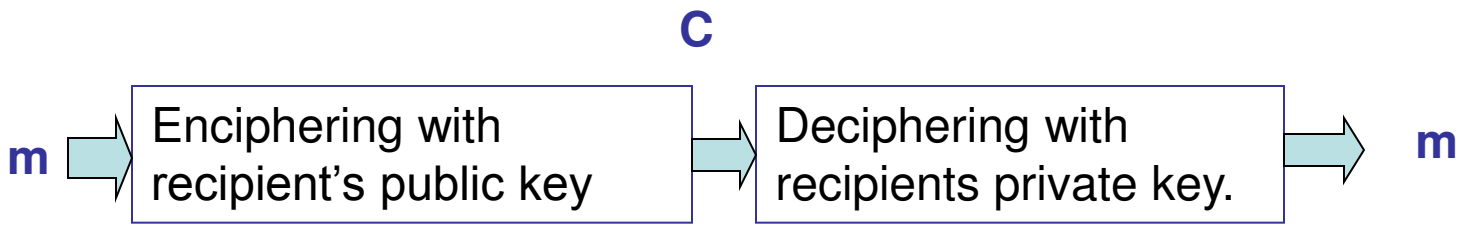
The answer is yes, in this trivial example, an intruder could easily guess the value of d. But a major concept of the RSA algorithm is to use very large numbers for d and e. In practice, the numbers are so large (on the scale of tens of digits) that the trial-and-error approach of breaking the code takes a long time (several years) even with the fastest computer today.

Selection of Public and Private Keys

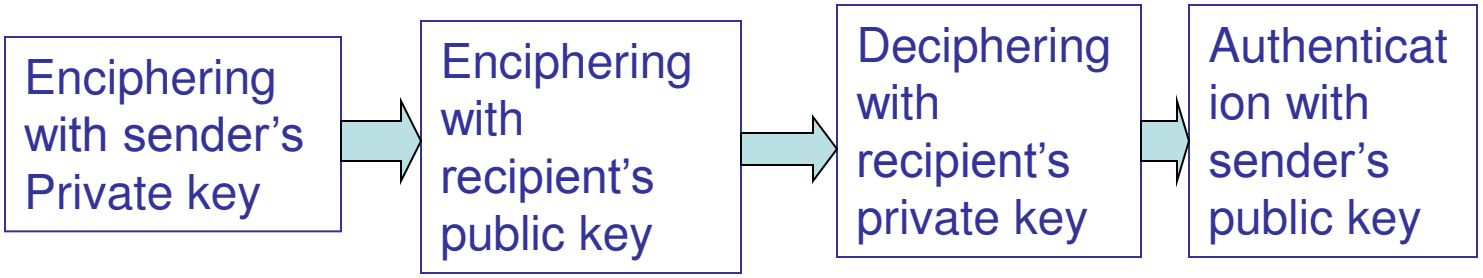
1. Choose two large prime numbers p and q.
2. Compute n= p x q.
3. Choose e (less than n) such that e and (p -1) (q -1) are relatively prime (having no common factors other than 1).
4. Choose d such that e x d mod [(p-1) (q-1)] is equal to 1.

Confidentiality and authentication together in RSA

1. ONLY CONFIDENTIALITY



2. BOTH CONFIDENTIALITY & AUTHENTICATION



How does RSA provide data and origin authentication?

Example: Let p=7, q= 11; so, **n = 77**. Let e= 17; so **d= 53**. Suppose, Allice wishes to send Bob "HELLO WORLD". The plaintext is 07 04 11 11 14 26 22 14 17 11 03. Using **Allice's private key(d, n)** , the ciphertext is

07^{53} mod 77 = 35

04^{53} mod 77 = 09 ….

or, 35 09 44 44 93 12 24 94 04 05.

Providing Confidentiality and Authentication by RSA

Providing both confidentiality and authentication requires enciphering with the **sender's private key and the recipent's public key.**

Example: Suppose, Allice wishes to send Bob HELLO WORLD in confidence and authenticated. Assume Allice's private key is 53 and Bob's public key is 37. The plaintext is 07 04 11 11 … and the encipherment is

$(07^{53} \bmod 77)^{37} \bmod 77 = 07$

$(04^{53} \bmod 77)^{37} \bmod 77 = 37$

or, 07 37 44 44 14 59 22 14 61 44 47.

Deciphering confidential and authenticated message

The recipient uses recipient's private key to decipher the message and the sender's public key to authenticate it.

Bob receives the ciphertext: 07 37 44 44 14 59 22 14 61 44 47. The decipherment is

$(07^{13} \bmod 77)^{17} \bmod 77 = 07$

$(37^{13} \bmod 77)^{17} \bmod 77 = 04$ ……

Or, 07 04 11 11 14 26 22 14 17 11 03.

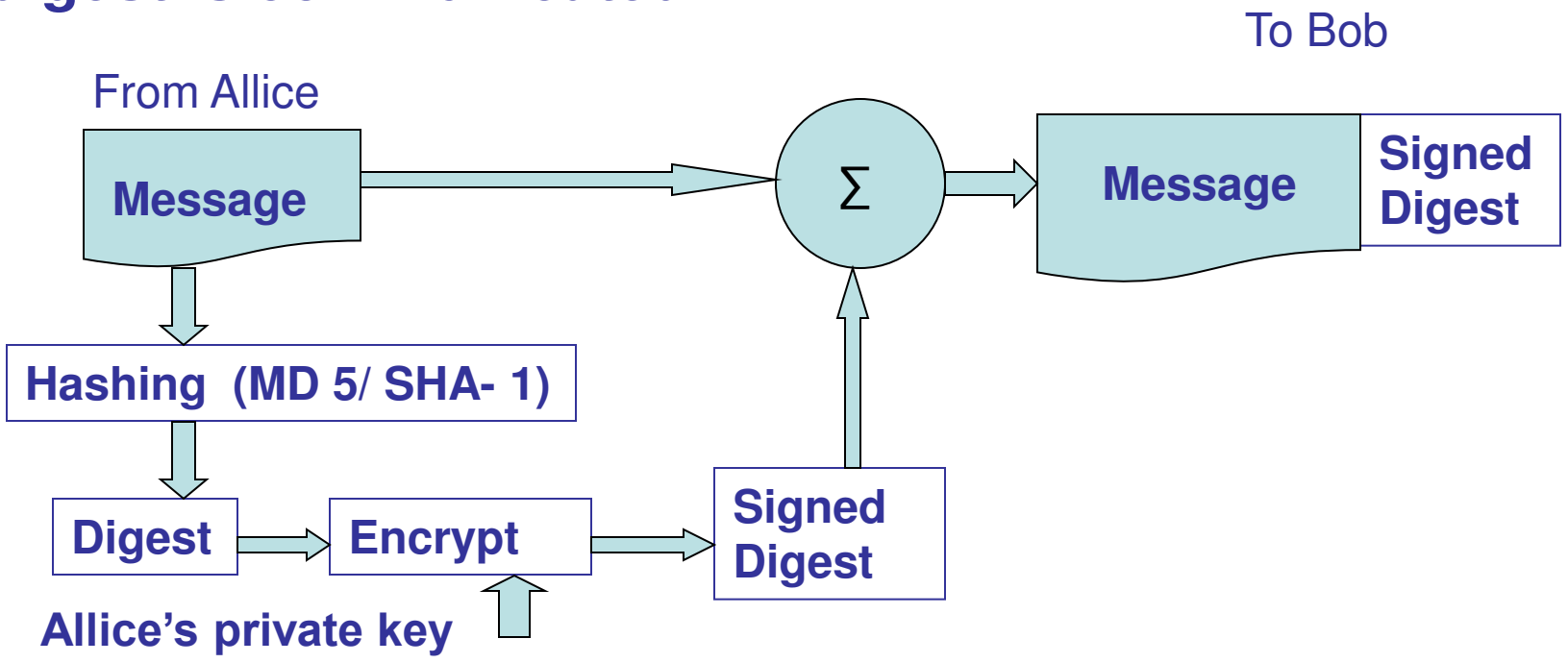
What is Digital Signature?

A digital signature ensures authentication (sender's identity), integrity (no changes in data) and non-repudiation (i.e. the receiver is able to prove that the received message came from a specific sender).

It can be realized by RSA through enciphering by sender's private key and deciphering by sender's public key.

Signing the Digest

Signing the entire message is not time-efficient. The sender prepares a digest by Hashing and then encrypts the digest. The message plus the signed digest is communicated.



Receiver Site