SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

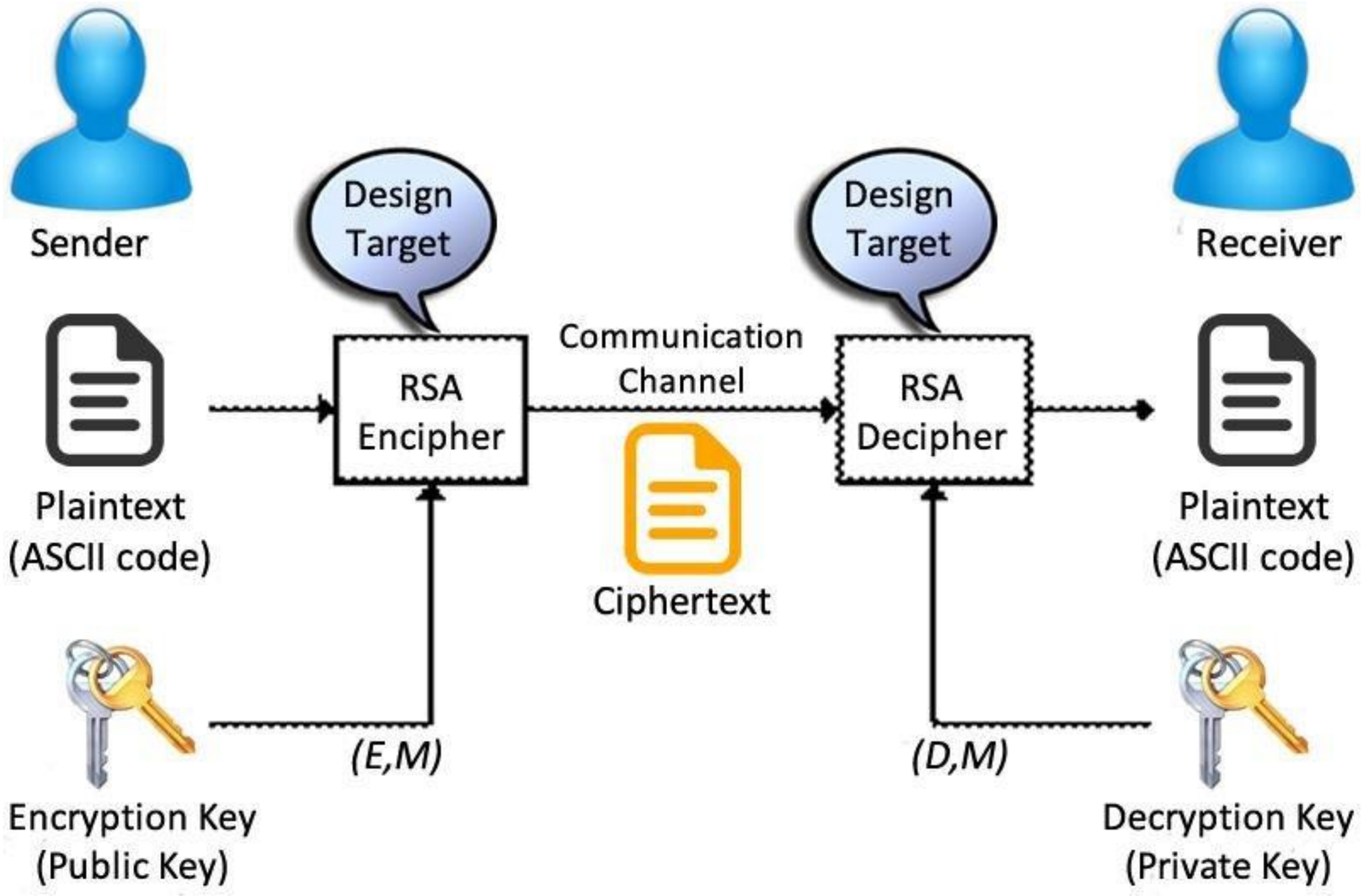
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME : 19CS503 Cryptography and Network Security

III YEAR /V SEMESTER

Unit 3- Public Key Cryptography

Topic : RSA Algorithm

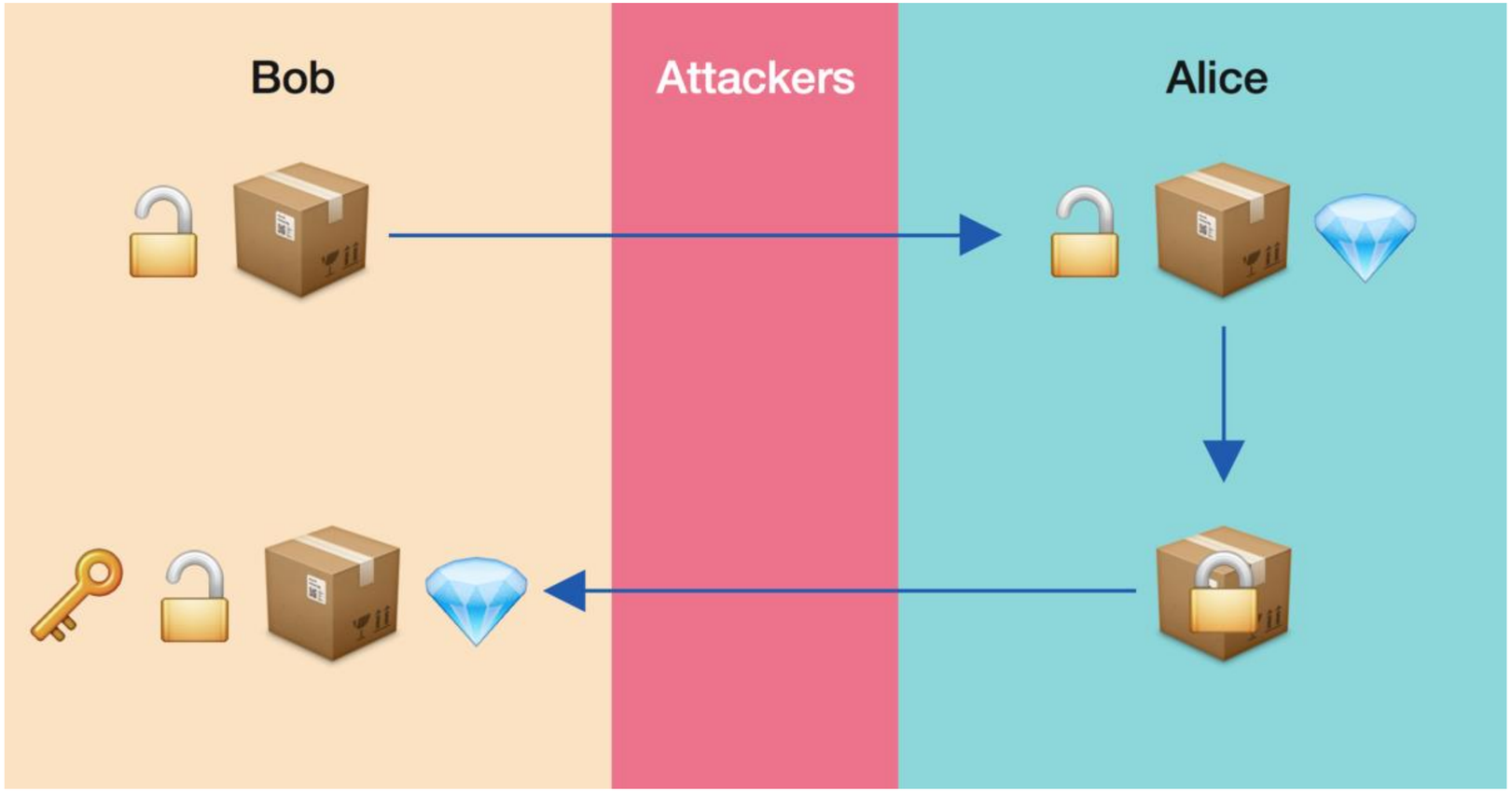

Sender
Design Target
Design Target
Receiver
Plaintext (ASCII code)
RSA Encipher
Communication Channel
RSA Decipher
Plaintext (ASCII code)
Ciphertext
(E,M)
(D,M)
Encryption Key (Public Key)
Decryption Key (Private Key)

public-key cryptography

Suppose Alice wishes to send Bob a valuable diamond, but the jewel will be stolen if sent unsecured. Both Alice and Bob have a variety of padlocks, but they don't own the same ones, meaning that their keys cannot open the other's locks.

How did Alice send the diamond to Bob?

public-key cryptography



public-key cryptography

1. Bob first sends Alice an unlocked padlock. Note that Bob would give anyone an unlocked padlock, as the only use for one is to send Bob something.

2.Alice adds Bob's lock and sends the package to Bob, and

3. Bob removes his lock and opens the package.

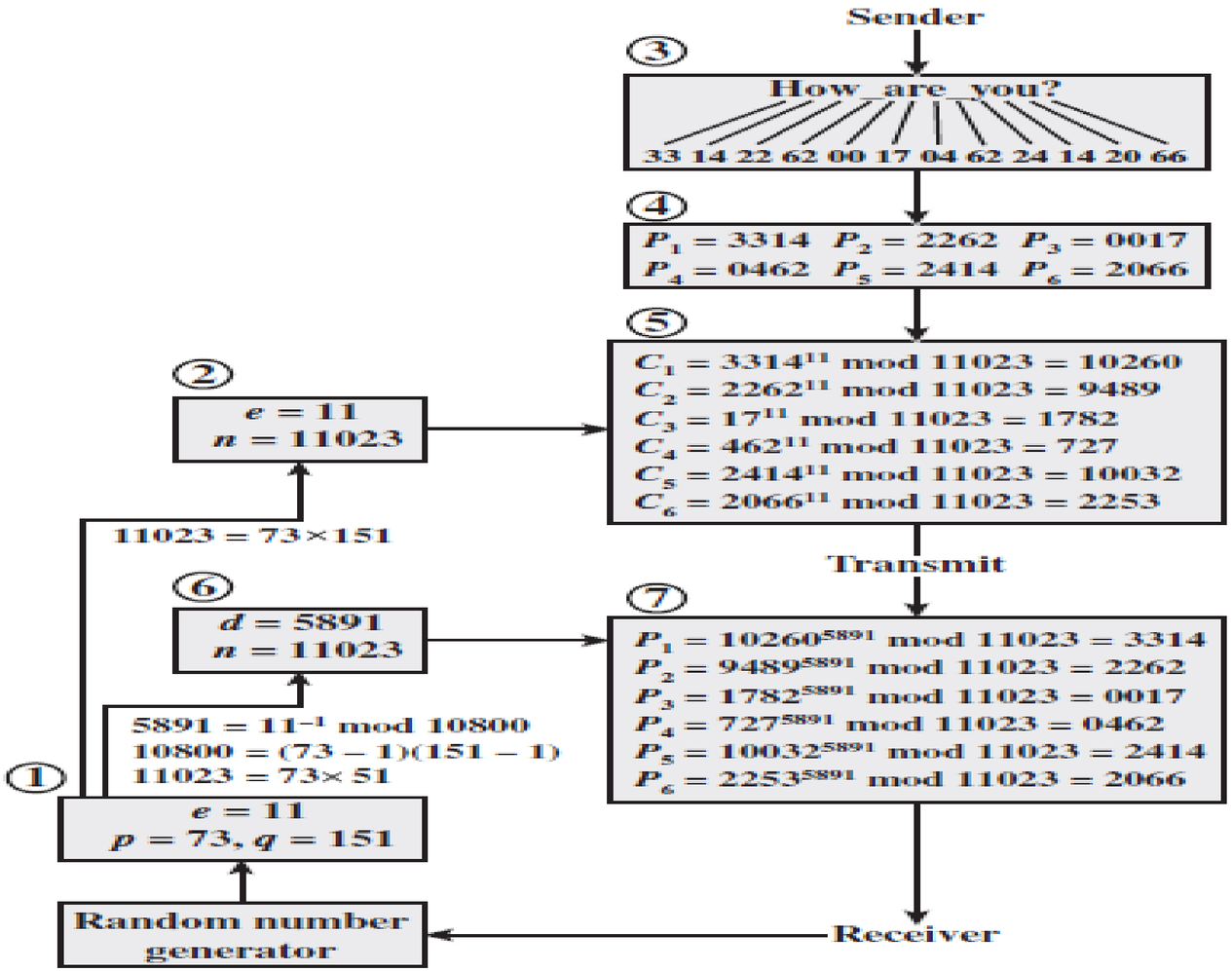
RSA

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

RSA

- **Encryption by Bob with Alice's Public Key**
  - Plaintext: $M < n$
  - Ciphertext: $C = M^e \ mod \ n$
- **Decryption by Alice with Alice's Public Key**
  - Ciphertext: C
  - Plaintext: $M = C^d \ mod \ n$

RSA EXAMPLE


Sender
3
How_are_you?
33 14 22 62 00 17 04 62 24 14 20 66
4
$P_1 = 3314$ $P_2 = 2262$ $P_3 = 0017$
$P_4 = 0462$ $P_5 = 2414$ $P_6 = 2066$
5
$C_1 = 3314^{11} \bmod 11023 = 10260$
$C_2 = 2262^{11} \bmod 11023 = 9489$
$C_3 = 17^{11} \bmod 11023 = 1782$
$C_4 = 462^{11} \bmod 11023 = 727$
$C_5 = 2414^{11} \bmod 11023 = 10032$
$C_6 = 2066^{11} \bmod 11023 = 2253$
2
$e = 11$
$n = 11023$
$11023 = 73 \times 151$
Transmit
6
$d = 5891$
$n = 11023$
7
$P_1 = 10260^{5891} \bmod 11023 = 3314$
$P_2 = 9489^{5891} \bmod 11023 = 2262$
$P_3 = 1782^{5891} \bmod 11023 = 0017$
$P_4 = 727^{5891} \bmod 11023 = 0462$
$P_5 = 10032^{5891} \bmod 11023 = 2414$
$P_6 = 2253^{5891} \bmod 11023 = 2066$
$5891 = 11^{-1} \bmod 10800$
$10800 = (73 - 1)(151 - 1)$
$11023 = 73 \times 51$
1
$e = 11$
$p = 73, q = 151$
Random number generator
Receiver

RSA Security

- possible approaches to attacking RSA are:
  - brute force key search - infeasible given size of numbers
  - mathematical attacks - based on difficulty of computing ø(n), by factoring modulus n
  - timing attacks - on running of decryption
  - chosen ciphertext attacks - given properties of RSA

REFERENCES

1. William Stallings, Cryptography and Network Security, 6 th Edition, Pearson Education, March 2013.

THANK YOU