

## SISTEME ASIMETRICE DE CRIPTARE

### Sistemul de Criptare RSA

#### I. Descrierea sistemului de criptare RSA.

#### II. Criptare

- i. Cheia publică a destinatarului este ( $N=44929$ ,  $e=171$ );
- ii. Criptați mesajul **CRİPTOGRAFIE ASIMETRICA**.

#### III. Decriptare

- i. Cheia voastră secretă este ( $p=131$ ,  $q=397$ ;  $d=34679$ );
- ii. Ați recepționat următorul mesaj:

**47651 # 22153 # 46384 # 48562 # 47651 # 17696 # 19353 # 10780 # 18597 # 09585 #  
48562 # 03433 # 43848 # 17696 # 48562 # 45881 # 42566 # 39329 # 09977 # 17696 #  
01575 # 48562 # 16514 # 10780 # 22153 # 46384 # 39329 # 01575 # 43848 # 48562 #  
03433 # 43848 # 50228 # 10780 # 09977 # 39329 # 46384**

- iii. Determinați textul clar;
- iv. Care este cheia cu care a fost criptat acest text?

#### IV. Factorizarea modului RSA

- i. Se consideră cheia publică ( $N=2244959$ ,  $e=14521$ );
- ii. Ați interceptat următorul text:

**2155762 # 0459375 # 0981116 # 1875481 # 1127556 # 0951877 # 1432972 # 1336907 #  
1164389 # 1164389 # 0399925 # 0625583 # 1147052 # 1103641 # 0132772 # 1749512 #  
1236454 # 1466948 # 2048761 # 1251360 # 2080806 # 0798210 # 1127556 # 0951877 #  
1147052 # 1544777 # 0017577 # 1971705 # 1181633 # 0431945 # 0362558 # 0514295 #  
2048761 # 0751861 # 0881088 # 0984236 # 0782785 # 1127556 # 1370155 # 0596103**

- iii. Puteți să îl decriptați?
- iv. Ce cheie secretă ați obținut?

### V. Coeficient de criptare mic

Observație: Nu folosiți descompunerea modulului!

- i. Bob are cheia publică ( $N=224718679$ ;  $e=3$ );
- ii. Acesta primește de la Alice mesajul **001030301**.
- iii. Care este mesajul trimis de Alice?

### VI. Coeficient de criptare mic și mesaje relaționate

Observație: Nu folosiți descompunerea modulului!

- i. Bob are cheia publică ( $N=908689$ ;  $e=3$ );
- ii. Acesta primește de la Alice mesajul criptat **110110**, despre care ați aflat că îi corespunde mesajului clar **082677**.
- iii. Bob primește apoi un nou mesaj criptat: **880880**.
- iv. Îl puteți decripta?

### VII. Atac cu text criptat ales

Observație: Nu folosiți descompunerea modulului!

- i. Lui Bob îi corespunde cheia publică ( $N=1418017$ ,  $e=5$ );
- ii. Ați interceptat mesajul criptat  $C = 0718257$  care îi era destinat lui Bob;
- iii. Reușiți să îl convingeți pe Bob să decripteze un singur mesaj criptat pe care i-l trimiteți, oricare în afară de  $C$  și să vă transmită rezultatul. În urma acestui pas veți deține o pereche de tip text clar – text criptat ales.
- iv. Ce mesaj îi dați lui Bob pentru a-l decripta, având în vedere că scopul vostru este de a decripta  $C$ ?
- v. Care este mesajul clar corespunzător lui  $C$ ?

### VIII. Texte clare invariabile

- i. În ce se va cripta textul clar 0, indiferent de cheia publică folosită?
- ii. Găsiți încă 2 exemple de astfel de mesaje.

## Sisteme de Criptare Hibridă

### I. Sisteme de criptare hibride.

### II. Criptare

- i. Alegeți un text oarecare.
- ii. Cripțați hibrid textul folosind opțiunea Crypt/Decrypt > Hybrid > RSA – AES Encryption.
- iii. Urmăriți fiecare pas.

### III. Decriptare

- i. S-a recepționat următorul mesaj:

52 65 63 65 69 76 65 72 3A 20 20 20 20 5B 53 69 64 65 43 68  
61 6E 6E 65 6C 41 74 74 61 63 6B 5D 5B 42 6F 62 5D 5B 52 53  
41 2D 35 31 32 5D 5B 31 31 35 32 31 37 39 34 39 34 5D 5B 50  
49 4E 3D 31 32 33 34 5D 20 20 20 20 20 4C 65 6E 67 74 68 20  
6F 66 20 65 6E 63 72 79 70 74 65 64 20 73 65 73 73 69 6F 6E  
20 6B 65 79 3A 20 20 20 20 35 31 32 20 20 20 20 45 6E 63 72  
79 70 74 65 64 20 73 65 73 73 69 6F 6E 20 6B 65 79 3A 20 20  
20 20 91 3C 62 89 E7 B7 6B 7D 94 92 74 44 C4 77 FF 2F F3 B6  
CA 22 18 33 EA 77 3E 2C 1D C4 0A 08 C8 B2 06 C9 19 C8 43 8D  
4C E9 6C 16 6B 5E BE DB 6F FF 07 B5 A6 CC 4A 72 22 46 3E F8  
B3 AD 4F CD 11 13 20 20 20 20 53 79 6D 6D 65 74 72 69 63 20  
6D 65 74 68 6F 64 3A 20 20 20 20 41 45 53 20 20 20 20 41 73  
79 6D 6D 65 74 72 69 63 20 6D 65 74 68 6F 64 3A 20 20 20 20  
52 53 41 20 20 20 20 43 69 70 68 65 72 74 65 78 74 3A 20 20  
20 20 BA B1 55 BF 21 F1 1C 84 98 11 75 9C 03 45 91 B5 8E 5C  
5A 5D 55 F9 73 9C 28 02 93 8F 18 92 8A 46 6D EF BB 80 6E 69  
A6 0C CF 70 78 01 6E F0 DB 2A C1 F6 9E 0D EC F5 25 DB 5F CE  
C0 DE 0B BD D3 A0 8C 59 1E DF CA 7E 0C FA 35 DC 6A 88 30 44  
9F 92 91 D3 A8 E6 82 AA 1B F6 53 A3 15 24 28 2C 0D 02 29 C7  
93 B5 6B 42 5D 34 C0 6D 93 6F D4 F6 38 08 4C E5 37 5F 20 32  
38 D9 93 AF 96 C6 5F E1 39 6A 17 4E 9D EC 67 B9 70 00 C1 FC  
07 EF B0 6A A9 83 17 46 29 28 CA 64 D7 A2 49 CB 22 FC 8F 1C  
BC 79

- ii. Mesajul a fost criptat folosind un sistem hibrid de tip AES – RSA și conține și cheia de sesiune criptată;
- iii. Decripțați mesajul. Folosiți drept cod al lui Bob 1234.

① Mai multe informații:

1. CrypTool Portal (Cryptool 1.4)

[www.cryptool.org/en](http://www.cryptool.org/en)

2. Mario Calagj - Laboratory Exercises II: Symmetric and Asymmetric Cryptography

<http://www.scribd.com/doc/48378086/Symmetric-Asymmetric-Cryptool>