# SISTEME ASIMETRICE DE CRIPTARE

## Sistemul de Criptare RSA

### I. Descrierea sistemului de criptare RSA.

### II. Criptare

i. Cheia publică a destinatarului este **(N= 35639, e= 541)**;
ii. Criptaţi mesajul **CRIPTOGRAFIE CU CHEIE PUBLICA**.

### III. Decriptare

i. Cheia voastră secretă este **(p= 137, q = 163; d= 20707)**;
ii. Aţi recepţionat următorul mesaj:

**02035 # 02224 # 05225 # 06201 # 18062 # 06073 # 11339 # 10629 # 01245 # 18742 # 05645 # 02224 # 12496 # 11339 # 04586 # 10312 # 20025 # 06201 # 05645 # 18742 # 07358**

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

### IV. Factorizarea modulului RSA

i. Se consideră cheia publică **(N= 1355839, e= 17611)**;
ii. Aţi interceptat următorul text:

**0401823 # 0166732 # 1144080 # 0468032 # 0836949 # 0624136 # 1085655 # 0063752 # 1275978 # 0861579 # 0136220 # 1145286 # 1046459 # 0367036 # 0178557 # 1085655 # 0212238 # 0213814 # 0213814 # 1225404 # 0557812 # 1280374 # 1043317 # 1009720 # 0039826 # 1273944 # 0624136 # 0674759 # 0729085 # 0138090 # 0468032 # 0728861 # 0557812 # 0511206 # 1203865 # 0610572 # 1333384 # 0945859 # 0674759 # 0034217 # 1244274 # 0111949 # 0405214 # 1148040 # 0272551 # 0071451 # 0468032 # 1224768**

iii. Puteţi să îl decriptaţi?
iv. Ce cheie secretă aţi obţinut?

## V. Coeficient de criptare mic

Observaţie: Nu folosiţi descompunerea modulului!

i. Bob are cheia publică **(N= 29291707; e=3);**
ii. Acesta primeşte de la Alice mesajul **01367631**.
iii. Care este mesajul trimis de Alice?

## VI. Coeficient de criptare mic şi mesaje relaţionate

Observaţie: Nu folosiţi descompunerea modulului!

**i.** Bob are cheia publică **(N= 2283217; e=3);**
ii. Acesta primeşte de la Alice mesajul criptat **0111111,** despre care aţi aflat că îi corespunde mesajului clar **0899776** .
iii. Bob primeşte apoi un nou mesaj criptat: **0888888**.
iv. Îl puteţi decripta?

## VII. Atac cu text criptat ales

Observaţie: Nu folosiţi descompunerea modulului!

i. Lui Bob îi corespunde cheia publică **(N=6952399 , e= 3);**
ii. Aţi interceptat mesajul criptat **C = 0001728** care îi era destinat lui Bob;
iii. Reuşiţi să îl convingeţi pe Bob să decripteze un singur mesaj criptat pe care i-l trimiteţi, oricare în afară de **C** şi să vă transmită rezultatul. În urma acestui pas veţi deţine o pereche de tip text clar – text criptat ales.
iv. Ce mesaj îi daţi 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. Găsiţi încă 2 exemple de astfel de mesaje.

## Sisteme de Criptare Hibridă

### I. Sisteme de criptare hibride.

### II. Criptare

i. Alegeţi un text oarecare.
ii. Criptaţi hibrid textul folosind opţiunea Crypt/Decrypt > Hybrid > RSA – AES Encryption.
iii. Urmăriţi fiecare pas.

### III. Decriptare

i. S-a recepţionat 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 16 5C 16 91 37 14 9F 51 1B 19 63 2C 01 C1 0D EE A2 23**
**56 E2 B4 2A 5B ED FB C3 1A A4 7A 95 B6 12 25 76 14 53 2A 33**
**00 99 47 11 B5 C5 F6 7F 7E B5 78 FB 40 E6 DA A7 5F 95 4F 82**
**AF 77 D4 F0 F6 6E 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 37 F3 0A 34 21 19 0F D2 56 AF 89 3F 4A 95 8C 46 10 DC**
**F1 1B AE 01 55 C5 66 84 D1 6B B6 24 64 8D 93 03 72 4B 0B 12**
**D2 72 91 22 E0 7A FD 27 B8 F8 2C 58 34 70 08 D2 04 37 48 D9**
**D9 92 11 F7 71 7A 83 91 63 6E 12 98 65 42 EA E2 60 C9 B1 81**
**3E 81 CA B2 61 9B 2A 21 F2 BB F6 AE 15 B7 81 B3 81 39 A9 7E**
**9A 48 48 AD 99 14 BE 84 EC 6A 49 37 9B 5E 0E F2 B4 85 0E 07**
**F1 E3 7D 4E CE 7D 01 86 D1 51 A0 D4 C8 F4 63 59 76 65 29 D1**
**E7 58 B0 8D BC 5D 60 06 F9 FD 09 4F 59 AC 98 1A 17 81 9D 0D**
**E4 53**

ii. Mesajul a fost criptat folosind un sistem hibrid de tip AES – RSA şi conţine şi cheia de sesiune criptată;
iii. Decriptaţi mesajul. Folosiţi drept cod al lui Bob 1234.

ⓘ Mai multe informaţii:

1. CrypTool Portal (Cryptool 1.4)
   www.cryptool.org/en
2. Mario Calagj - Laboratory Exercises II: Symmetric and Asymmentric Cryptography
   http://www.scribd.com/doc/48378086/Symetric-Asymmetric-Cryptool