SISTEME ASIMETRICE DE CRIPTARE

Sistemul de Criptare RSA

I. Descrierea sistemului de criptare RSA.

II. Criptare

i. Cheia publică a destinatarului este **(N= 32743, e= 321)**;
ii. Criptaţi mesajul **CRIPTOGRAFIE CU CHEIE PUBLICA**.

III. Decriptare

i. Cheia voastră secretă este **(p= 149, q = 151; d= 16451)**;
ii. Aţi recepţionat următorul mesaj:

15565 # 00491 # 22078 # 21241 # 01415 # 02806 # 09480 # 05972 # 01667 # 10389 # 11189 # 00491 # 21908 # 09480 # 15618 # 17387 # 14932 # 21241 # 11189 # 10389 # 06603

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= 774689, e= 32141);**
ii. Aţi interceptat următorul text:

537717 # 071605 # 492170 # 400948 # 388049 # 105330 # 622685 # 770293 # 557240 # 333677 # 311770 # 079862 # 601675 # 342120 # 695232 # 622685 # 196201 # 616260 # 616260 # 194268 # 363347 # 607975 # 375366 # 074826 # 174279 # 280724 # 105330 # 224310 # 328670 # 153023 # 400948 # 634910 # 363347 # 767169 # 038909 # 029105 # 157990 # 664291 # 224310 # 029796 # 629614 # 254592 # 419178 # 502672 # 241425 # 309727 # 400948 # 428933

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= 28049599; e=3);**
ii. Acesta primeşte de la Alice mesajul **000027000**.
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= 3521017; e=3);**
ii. Acesta primeşte de la Alice mesajul criptat **0001111,** despre care aţi aflat că îi corespunde mesajului clar **0108561** .
iii. Bob primeşte apoi un nou mesaj criptat: **0008888**.
iv. Îl puteţi decripta?

VII. Atac cu text criptat ales

Observaţie: Nu folosiţi descompunerea modulului!

i. Lui Bob îi corespunde cheia publică **(N=4399357 , e= 3);**
ii. Aţi interceptat mesajul criptat **C = 4348266** 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 66 83 E3 65 51 34 0E 63 45 41 22 66 8A 08 A6 D1 8B 35
B9 0D 68 2F D9 C0 E5 FA 48 B9 25 96 1A FB AC 22 2D B1 9B 66
27 A9 E9 54 47 EE 68 C1 4D 43 49 E0 27 B0 A5 C1 6E 8C AB 60
DE C4 10 6D 36 0D 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 76 E2 93 52 FE 4B 1C 27 00 F5 45 CD CE C4 DB 0F CA 15
F3 F0 2F 85 3B 4F C1 56 30 6C 20 B6 3A 96 2B FA BA FF C8 49
90 8E 44 A8 91 E2 AE 26 1F C9 E5 94 F9 9D 6C 7E BF 99 31 EC
8C 10 96 8C A2 CD CB A6 A2 AE A2 9B DD 83 FB FB 07 FF 5B 4D
8B CE FC 18 82 C5 34 D2 A5 70 4F C8 C0 9A B6 BF 0A 07 2C 40
EC 5C A2 8E 84 D3 44 4B E7 1B 51 2F 24 82 6D C1 9A 22 8A 9E
B4 22 B4 07 B4 4D B2 87 2E D3 01 2F 70 F4 F0 55 BE DE 09 33
31 18 D0 D8 FE 86 85 FF D0 9C AE A7 EE 16 E3 67 74 C7 7F BE
E9 82

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