1

A

$d_B = e_B^{-1} \bmod (p-1)(q-1)$

Alice weet p, q en e_B dus d_B kan worden berekend.

B

$\gcd(e_a,e_b) = 1$

We hebben x en y zodat: $x * e_a + y * e_b = 1$.

Als $\gcd(e_a, e_b) = 1$ dan zijn e_a en e_b copriem.

We weten verder dan x en y priem zijn, dus $\gcd(x, y) = 1$.

Hierdoor kunnen we x en y vinden met het Euclidian algoritme. Als we x en y weten kunnen we C_a en C_b decrypten naar M_a en M_b.

2

A

We hebben certificate C_Q^P nodig, Q weet de publieke sleutel van P dus kan hij nagaan of het certificate klopt.

B

Hier hebben we de twee andere certificates voor nodig, S moet haar private sleutel gebruiken als we een signed bericht naar Q willen sturen. Hiervoor zijn twee certificates nodig: C_R^P en C_S^R. Dit omdat Q de publieke sleutel van R niet heeft en daarom is het certificate C_R^P.

3

Informatie:

n = 902140983721750316999465244309489804973 3

e = 65537

RSA(r) = 897216349798731473416999902520226187144 5

Session key = 128 bit AES key

Ciphertext:

4A 20 EF EE 84 F3 85 BD 00 2D 5B DF 3F 2B F0 C2

9B F0 B3 18 74 6A 08 78 96 13 3D CE D9 17 B7 4F

69 5A 8F 72 B2 71 59 36 EC D5 E7 55 54 3C C3 BB

IV: 55 BB 82 09 2A 18 AA A9 EF 68 0A 6C 2C 94 8F 00

De session key kan gevonden worden door SHAKE(128) toe te passen op waarde r.

Waarde r kan gevonden worden door de RSA encryptie over RSA(r) te breken.

We hebben p en q nodig zodat p * q = n.

Met een zelfgeschreven programma p en q gevonden:

P = 81676168843571580071

Q = 110453391300656531123

Met wolfram-alpha de sleutel d berekend door e, p en q te gebruiken:

D = 25110786006457679299256545528600045931l3

R kan nu worden berekend door rsa(r)^d mod n te berekenen, dit geeft:

r = 764455618499694837023660604902451650l3

Nu kunnen we shake128 op r toepassen, dit geeft:

AES Key: 1E 2E 38 B0 8D 69 C3 9B 44 9F A2 14 F7 D5 DA A2

Ciphertext:

4A 20 EF EE 84 F3 85 BD 00 2D 5B DF 3F 2B F0 C2

9B F0 B3 18 74 6A 08 78 96 13 3D CE D9 17 B7 4F

69 5A 8F 72 B2 71 59 36 EC D5 E7 55 54 3C C3 BB

Hierna kunnen we met de AES key en de Ciphertext de plaintext berekenen:

Dit:

4A 20 EF EE 84 F3 85 BD 00 2D 5B DF 3F 2B F0 C2

9B F0 B3 18 74 6A 08 78 96 13 3D CE D9 17 B7 4F

69 5A 8F 72 B2 71 59 36 EC D5 E7 55 54 3C C3 BB

Wordt:

01 D3 E7 29 67 79 CD C0 8C 48 5D 03 5E F0 FC 20

2B 52 8A CE D7 82 F0 D8 61 40 32 AC 57 0B BF B1

E8 99 D5 6A 15 0D 6D 20 CE 4B 65 96 81 4F EF 17

Dit is de plaintext na de AES decryptie, nu moeten we nog een XOR toepassen:

01 D3 E7 29 67 79 CD C0 8C 48 5D 03 5E F0 FC 20

XOR

55 BB 82 09 2A 18 AA A9 EF 68 0A 6C 2C 94 8F 00

=

54 68 65 20 4D 61 67 69 63 20 57 6F 72 64 73 20

4A 20 EF EE 84 F3 85 BD 00 2D 5B DF 3F 2B F0 C2

XOR

2B 52 8A CE D7 82 F0 D8 61 40 32 AC 57 0B BF B1

=

61 72 65 20 53 71 75 65 61 6D 69 73 68 20 4F 73

E8 99 D5 6A 15 0D 6D 20 CE 4B 65 96 81 4F EF 17

XOR

9B F0 B3 18 74 6A 08 78 96 13 3D CE D9 17 B7 4F

=

73 69 66 72 61 67 65 58 58 58 58 58 58 58 58 58

Nu hebben we de plaintext gecodeerd in ASCII:

Plaintext(ASCII) = 54 68 65 20 4D 61 67 69 63 20 57 6F 72 64 73 20

61 72 65 20 53 71 75 65 61 6D 69 73 68 20 4F 73

73 69 66 72 61 67 65 58 58 58 58 58 58 58 58 58

Als we dit converteren naar normale taal dan is dit de plaintext:

The Magic Words are Squeamish OssifrageXXXXXXXXX