MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

RSA: Two different Keys – Same Ciphertext

Authors: Verena Brunner, Bernhard Esslinger

August 2011 (Update August 2018)

Introduction

In one of your courses you got the task to send RSA encrypted messages to your course participants. Every participant has his own key pair. All public keys are known by every course member and by you. You want to send the same message encrypted with the different public exponents to every participant.

You encrypt the message using every single public key. Wait, you already know this ciphertext. Actually, two colleagues have chosen the same modulus n by accident. However, their public keys e are different. Nevertheless, the message encrypted with the two different keys leads to the same ciphertexts.

Modulus = 6A163
Plaintext: OK
The ciphertext encrypted with e_1=1E437 is 57A27.
The ciphertext encrypted with e_2=35A47 is 57A27.

This challenge should draw your attention to two special features of RSA

a) The scenario of the introduction shows the following: Two recipients happen to have the same modulus n, but different public keys e. They will both receive the same message m in encrypted form. This is not only conspicuous but also dangerous: If an attacker who knows the public keys catches the associated ciphertexts c_1 and c_2, he can use the extended Euclidean algorithm to determine the plaintext message m without factoring n and without knowing the private key d.

b) The scenario of this challenge is slightly different: Again, the two recipients happen to have the same modulus n with different public keys e_1 and e_2. But this time, different messages m_1 and m_2 will be sent to them. What is special here is that the same bijective assignment m_i to c_i $\forall$ m_i can be generated by more than one pair (e, d), and that there can even be more than one matching e to a d.

Assignment (1/2)

The assignment consists of two parts:

1. First, identify the smallest value d to decrypt all ciphertexts that were generated using e_1 and e_2. Use the modulus n and the two public exponents to obtain this value.
2. Afterwards, use this special value d to decrypt two ciphertexts. You were able to catch these two different ciphertexts, which result in different plaintexts, from other course members. One ciphertext is encrypted with the public key e_1, the other one is encrypted with the public key e_2.

Assignment (2/2)

Public keys of the receivers:
e_1= 1E437 and e_2= 35A47, each with the same modulus = 6A163

A ciphertext of your colleague encrypted with the public key e_1:
12306 # 40C3F

Another ciphertext now encrypted with the public key e_2:
15434 # 370AE

The solution consists of the hexadecimal value of d and the two different plaintexts as a readable text (all in a row, without blanks).
Example: d = A12F3, plaintext1 = LEMON, plaintext2 = TREE
$\rightarrow$ Sample solution: A12F3LEMONTREE

A Small Example with Numbers (1/2)

A hint to solve the first part of this challenge: If the factorization is done, you can compute $\varphi(n)$ and the lcm (least common multiple).

Modulus $n = 35 = 5 \cdot 7$, $\varphi(n) = 24$, $\mathrm{lcm}(p-1, q-1) = 12$

For $n = 35$, the two different public keys $e_1 = 5$ and $e_2 = 17$ create for all input values exactly the same output values (ciphertexts).

The table below illustrates the ciphertexts of all possible messages encrypted with the public key $e_1 = 5$:

m	0	1	2	3	4	5	6	7	8	9	10	11
m^5 mod 35	0	1	32	33	9	10	6	7	8	4	5	16
m	12	13	14	15	16	17	18	19	20	21	22	23
m^5 mod 35	17	13	14	15	11	12	23	24	20	21	22	18
m	24	25	26	27	28	29	30	31	32	33	34	
m^5 mod 35	19	30	31	27	28	29	25	26	2	3	34	

A Small Example with Numbers (2/2)

The following table contains the results for $e_2 = 17$:

m	0	1	2	3	4	5	6	7	8	9	10	11
$m^{17} \bmod 35$	0	1	32	33	9	10	6	7	8	4	5	16
m	12	13	14	15	16	17	18	19	20	21	22	23
$m^{17} \bmod 35$	17	13	14	15	11	12	23	24	20	21	22	18
m	24	25	26	27	28	29	30	31	32	33	34	
$m^{17} \bmod 35$	19	30	31	27	28	29	25	26	2	3	34	

Additional Information: Cryptographic Relevance

The special attack concerning the scenario of the introduction is only successful if the communication partners share one common modulus and if both ciphertexts (from the same plaintext message) are also identical. In reality, the primes for RSA are generated randomly and they have a size of about 1024 bit. Hence, the probability that both recipients generate the same primes and so the same modulus is used more than once is extremely small. There are so many primes of this size that it would not even be possible to store a list of them.

Additional Information: Uniqueness of e and d?

For a given RSA modulus n (and thus uniquely determined primes p and q) and for a given decryption exponent d, there are at least 2 different encryption exponents e, all making the same ciphertext from the same plaintext (i.e. they deliver the same permutation of values $m^i \bmod n$ $\forall i \in \{0, \ldots, n-1\}$). One can also say that there are at least two pairs (e_1,d_1) and (e_2, d_2) for each permutation, which generate the same ciphertext from the plaintext, and vice versa.

Therefore, the encryption exponent e is not unique. If we denote the smallest one with e, the whole set of values $e + \mathrm{lcm}(p-1, q-1)$ leads to the same result (where $e + k * \mathrm{lcm}(p-1, p-1) < \varphi(n)$ should apply). It's just a good habit to choose the smallest one as e.

The safety of RSA is not affected by this number-theoretic fact, because for practically used n (in the size of about 2048 bit) there are both sufficiently enough and sufficiently few different d.

Further details can be found e.g. within the CrypTool book, 12th edition.

Hint: Converting hex to integer

So that you can compare whether your conversion is correct, here is the corresponding partial solution for the public keys and the given ciphers:

$n = 0x6a163 = 434531$

$e_1 = 0x1e437 = 123959$
Ciphertext $C = 12306 \# 40C3F = 74502 \# 265279$

$e_2 = 0x35a47 = 219719$
Ciphertext $C = 15434 \# 370ae = 87092 \# 225454$