MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Broadcasting and low exponent – RSA-Attack

Authors: Verena Brunner, Bernhard Esslinger, Joerg-Cornelius Schneider

July 2011

Introduction

The asymmetric encryption scheme RSA is already more than 30 years old but still the best known and most commonly used public-key cryptosystem.
Nevertheless, certain configuration properties have to be kept in mind to obtain an appropriate amount of security. Unfortunately, some of these properties have not been considered in the following scenario.

A circular was encrypted with RSA for three different recipients. You were able to catch the following three ciphertexts.

Ciphertexts

C1 :

34d2fc2fa4785e1cdb1c09c9a5db98317d702aaedd2759d96e8938f740bf982e
2a42b904e54dce016575142f1b0ed112cc214fa8378b0d5eebc036dc7df3eeea

C2 :

3ddd68eeff8be9fee7d667c3c0ef21ec0d56cefab0fa10199c933cffbf0924d4
86296c604a447f48b9f30905ee49dd7ceef8fc689a1c4c263c1b3a9505091b00

C3 :

956f7cbf2c9da7563365827aba8c66dc83c9fb77cf7ed0ca225e7d155d2f573d
6bd18e1c18044cb14c59b52d3d1f6c38d8941a1d58942ed7f13a52caccc48154

The same message was sent encrypted to three business partners. In addition to the ciphertexts above, certificates (see additional file *mtc3-brunner-01-rsacrt.zip*) are available. These certificates contain the public exponents and the moduli of the three business partner.

There is no further information necessary to decrypt the original message because the three business partners are all using the same public key 3.

Your task is to use the Chinese remainder theorem to decrypt the ciphertext of the circular. Therefore, it is neither necessary to factorize the modulus nor to find a private key. Please send us the plaintext of the circular with blanks and special characters.

Information:
Of course, various methods exist to avoid such attacks in reality. For example, one recommendation in the PKCS#1 standard is to concatenate the message with pseudorandom bits before encrypting the message. Hence, the described attack is not successful anymore.