MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

SMARTCARD RSA

Author: Chair for Cryptology and IT Security
Ruhr-University Bochum

October 2010

RSA-CRT

SmartCrypto Inc. offers a smart card for secure RSA decryption. Since resources are very scarce on the chip, the chief engineer decided to use RSA-CRT with small values d_p and d_q. In RSA-CRT the decryption is done by first computing $m_1 = c^{d_p} \bmod p$ and $m_2 = c^{d_q} \bmod q$, and finally combining m_1, m_2 using the Chinese Remainder Theorem to obtain $m = c^d \bmod N$.

Challenge

Find the secret key corresponding to the given public parameters (N,e) and decrypt the message (*ciphertext*) given in the additional file (*mtc3-kitrub-05-smartcard.txt*) to this challenge.

The solution to this challenge is the first two words of the plaintext message.