MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Alice's Birthday Party – Part 1

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

October 2010 (Update: February 2014)

Scenario

Alice invites her friends Bob and Bertha to her birthday party. Naturally, she uses an encrypted email. Eve, however, did not get invited, but she eavesdropped on the encrypted emails intended for Bob and Bertha. Based on the public certificates of Bob and Bertha, Eve extracted their corresponding public keys (N, e_1) and (N, e_2). Eve then noticed that Bob and Bertha use the same modulus N.
Can Eve decrypt the messages with this information?

Encryption Method

Eve knows that Alice, Bob, and Bertha use a plain RSA encryption, where an RSA message m is encrypted such that $c = m^e \bmod N$. The RSA message m is constructed from the plaintext as follows: The first step is a base64 encoding. Then, the ASCII codes of the characters of the base64 string are concatenated and interpreted as hexadecimal integer. The decimal value of this integer is thus the RSA message m. The plaintext is short enough to guarantee $m < N$.

Example

For example, the text “Beispieltext” is encrypted as follows:
Base64(“Beispieltext”) = ”QmVpc3BpZWx0ZXh0”
Converting this value into ASCII codes results in
516d5670633342705a5778305a586830.
This corresponds to the integer
108235181207639582495826983402300008496.
And the ciphertext is thus
$c = 108235181207639582495826983402300008496^e \bmod N$.