Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Information Technology
FH Zentralschweiz

Public Key Cryptography - Exercise I

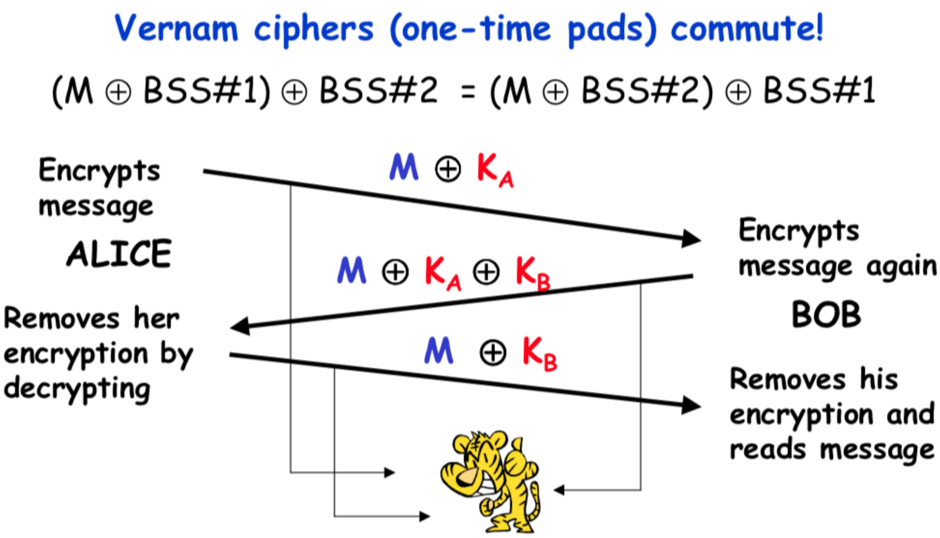
Prof. Dr. Josef F. Bürgler

I.BA_AAIS, Semesterweek 05

Please write down to solution of the exercises in a consise but comprehensible way. Numerical results should be accurate to 4 digits. Sketches should be correct qualitatively. At least 75% of the exercises have to be solve satisfactorily. Due time is one week after we have discussed the corresponding topic in class.

1 Shamir's three-pass protocol

Alice and Bob want the implement Shamir's three-pass protocol using the Vernam cipher, i.e. one-time pad. This is supposed to provide perfect secrecy. Is the following protocol secure?



Your Task: Can You compute the message? Make an example with $M = 010110111101$, $K_A = 101101110100$, and $K_B = 001011011011$.

2 Diffie Hellman

Alice and *Bob* agree to use $n = 13$ and $e = 11$. Alice chooses her secret number $a = 5$, whereas Bob chooses $b = 7$.

Your Task: What are the requirements for n and e? Are they fullfilled? Describe the key agreement protocol step by step using the above assumptions about a and b. What is the common secret key?

3 Discrete Logarithm Problem

Assume Mallory intercepts the message $A = 9$ from Alice to Bob and $B = 3$ from Bob to Alice. He also knows $n = 13$ and $g = 11$.

Your Task: Suppose Mallory wants to know the common key. Describe his steps to find this key!

4 Attack on textbook RSA

The public key $(n,e) = (2537,13)$ was used to encrypt the plaintext M. Eve intercepts the ciphertext $C = 2081$.

Your Task: Show how Eve computes the plaintext M!

5 Attack on textbook RSA — small exponent e

Frequently, the exponent e in the public key (n,e) is choosen very small, say $e = 3$. Hence, encryption of m is very fast

$$c = m^3 \bmod n$$

because modular exponentiation with small exponent is fast.
Unfortunately, this is is bad, if a small message, $m < n^{(1/3)}$ is encrypted, because there is no modular reduction and the attacker only has to compute the cubic root of c.
In the sequel we construct an attack which works for arbitrary messages m, $(1 < m < n-2)$.
To this end, we assume $e = 3$ and send the same message to three people with public keys (n_1,e), (n_2,e), and (n_3,e):

$$c_1 = m^3 \bmod n_1, \qquad c_2 = m^3 \bmod n_2, \qquad c_3 = m^3 \bmod n_3.$$

Furthermore we assume, that the moduli n_1, n_2, and n_3 are pairwise co-prime, i.e. $\gcd(n_i,n_j) = 1$ for $i \neq j$.

According to the chinese remainder theorem (CRT), there is a solution to these three linear congruences

$$m^3 = c_1 \bmod n_1, \qquad m^3 = c_2 \bmod n_2, \qquad m^3 = c_3 \bmod n_3.$$

First let $n = n_1 n_2 n_3$ and

$$N_1 = \frac{n}{n_1} = n_2 n_3, \qquad N_2 = \frac{n}{n_2} = n_1 n_3, \qquad N_3 = \frac{n}{n_3} = n_1 n_2.$$

Because n_i and n_j are co-prime if $i \neq j$, it follows that $\gcd(n_i, N_i) = 1$. Consequently, we can compute the (multiplicative) inverse y_i of N_i modulo n_i such that

$$N_1 y_1 \equiv 1 \pmod{n_1}, \qquad N_2 y_2 \equiv 1 \pmod{n_2}, \qquad N_3 y_3 \equiv 1 \pmod{n_3}.$$

Then the simultaneous solution of the system of linear congruences is

$$m^3 = \sum_{i=1}^{3} c_i N_i y_i \;=\; c_1 N_1 y_1 + c_2 N_2 y_2 + c_3 N_3 y_3.$$

Here m^3 is unique up to a multiple of $n_1 n_2 n_3$. Because m^3 is typically smaller than $n_1 n_2 n_3$ we can just take the cube root of m^3 to find m.

Your Task: Assume the message m is sent to 3 different people using textbook RSA, with moduli $n_1 = 377$, $n_2 = 391$, and $n_3 = 589$. You get hold of the corresponding ciphertexts

$$\begin{aligned} 330 &= m^3 \bmod 377 \\ 34 &= m^3 \bmod 391 \\ 419 &= m^3 \bmod 589 \end{aligned}$$

Compute $m = \sqrt[3]{x}$ using the CRT, where $x = m^3$ satisfies the system of linear congruences

$$\begin{aligned} x &\equiv 330 \pmod{377}, \\ x &\equiv 34 \pmod{391}, \\ x &\equiv 419 \pmod{589}. \end{aligned}$$

Use python in a Jupyter notebook. Use the (extended) Euklidean algorithm to compute the inverses and find or invent a python code, which implements the CRT.

6 Attack on textbook RSA — common module n

Suppose the CTO of a company wants that all employees use the same module n. The individual employees have pairwise different (e_i, d_i). Suppose, two employees A and B have the public keys (n, e_A) and (n, e_B) where $\gcd(e_A, e_B) = 1$.

Now the administration sends the encrypted message m to the two employees

$$c_A = m^{e_A} \bmod n \qquad\qquad c_B = m^{e_B} \bmod n$$

We will now show, that Eve is able to compute m if she knows the two ciphertexts c_A and c_B. She first computes a and b such that

$$ae_A + be_B = 1$$

She does it using the extended Euclidean algorithm which works because $\gcd(e_A, e_B) = 1$. Then she computes

$$\begin{aligned} c_A^a c_B^b &\equiv (m^{e_A})^a (m^{e_B})^b \\ &\equiv m^{ae_A + be_B} \equiv m^1 \equiv m \end{aligned}$$

Hence, as promised, she can compute m.

Your Task: Design a example with small numbers which demonstrates, this attack! Assume $n = 11 \cdot 13$, i.e. $p = 11$ and $q = 13$.

7 Elgamal

The prime number $p = 13$ and the generator $g = 3$ was used. Check if 3 is a genarator: otherwise use the next larger number after 3. Bob chooses the secret key $\mathrm{sk}_B = j = 3$ and Alice $\mathrm{sk}_A = i = 4$.

Your Task: Compute all intermediate results if Alice wants to securely send the message $m = 12$ to Bob.

Exercise 8: Elgamal

Alice uses the private key $a = 1751$ and computes the public key $(p = 2357, \alpha = 2, \alpha^a = 1185)$. Now Bob wants to encrypt the message $m = 2035$. He uses the random $k = 1520$.

Your Task: Compute the encrypted message and show how Alice decrypts the message.

Have fun with crypto!