Exercises for the course
Cryptography and Network Security

[Exercise II]

carl.bootland@esat.kuleuven.be

Public Key Cryptography

I. General Exercises

1. Compute $9^9 \bmod 133$ using repeated squaring.

   Extra: Compute $9^3 \bmod 133$, what can you deduce about $\lambda(133)$ without factoring 133? (Recall that for a positive integer n we have $a^{\lambda(n)} \equiv 1 \mod n$ for all a coprime to n.)

2. Compute efficiently $\varphi(100)$.

3. Compute $10^{82} \mod 33$ without using repeated squaring. Is 33 a strong pseudoprime to the base 10?

4. Compute $\gcd(1624, 6363)$.

5. Compute $101^{-1} \bmod 195$

6. Compute $5^{-1} \bmod 8$ using Euler's generalisation of Fermat's Theorem.

   Extra: What are the inverses of 3 and 7 modulo 8? Deduce the value of $\lambda(8)$? (In general, the Carmichael function of n, denoted $\lambda(n)$, is defined to be the minimal natural number λ such that $a^\lambda \equiv 1 \mod n$ for all a coprime with n.)

7. Find the smallest non-negative solution to the following system of congruences:

$$\begin{aligned} x &\equiv 4 \mod 19 \\ x &\equiv 7 \mod 11 \\ x &\equiv 1 \mod 7. \end{aligned}$$

II RSA encryption and decryption

1. (a) Consider an RSA encryption-system with modulus $n = 629 = 37 \cdot 17$. Choose the smallest possible public exponent. What is the corresponding secret exponent?

   (b) Calculate the ciphertext for the message '591'. Is there a problem?

   (c) Decrypt your result using the Chinese Remainder Theorem; verify whether you retrieve the plaintext.

   (d) Is it a problem to have a common modulus for RSA? That is, suppose a message m is encrypted with both of the public keys (n, e) and (n, f), with $\gcd(e, f) = 1$, then can you break RSA given these two ciphertexts $c_e = m^e \mod n$ and $c_f = m^f \mod n$. If so, how? (Hint: The Extended Euclidean Algorithm allows one to find integers x and y such that $\gcd(a, b) = xa + yb$.)

   (e) Is a small public exponent e a security problem? Why? (Hint: Suppose an entity wishes to send the same message m to three entities whose public moduli are n_1, n_2, n_3, and whose encryption exponents are all $e = 3$.)

2. Prove that if $n = pq$ is a product of two primes, then determining $\varphi(n)$ is equivalent to factoring n.

Extra Questions on RSA

3. Suppose you have somehow gained access to the decryption device of a competitor who is using the basic RSA encryption scheme. You notice that their decryption times are extremely fast and you suspect their decryption exponent d is very small. You know that their public key is $(e, n) = (31, 247)$ and have intercepted the ciphertext $c = 23$. Decrypt c without factoring n.

4. You are told that the ACME RSA software builds an RSA modulus by choosing a random k-bit prime p and setting q to be the smallest prime larger than p. You manage to get hold of an RSA public key $(e, n) = (1921, 141367)$ and a ciphertext $c = 70918$ of someone using the ACME software. Decrypt the ciphertext.

III ElGamal

1. Given $p = 89$, $a = 3$, $y = 69$. Verify for a message $m = 77$ whether the signature $(r, s) = (66, 77)$ is a valid signature.

2. Show that a different random number k must be selected for each message signed; otherwise the private key x can be determined with high probability.