Faculty of Computer Science and Engineering
Ho Chi Minh City University of Technology

CRYPTOGRAPHY AND NETWORK SECURITY

Lab 3 – RSA Algorithm

Nguyen Phuong Vuong - 1614186

Exercise 1.

What are the roles of the public and private key?
A user's private key is kept private and known only to the user. A user's public key is made available to others to use. The private key is able to create a signature that validates correctly the recipient. The public key can be used to encrypt information that can only be decrypted by the recipient's private key.

Exercise 2.

What is a one-way function?
A one-way function is one that maps domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy whereas the calculation of inverse is infeasible.

Exercise 3.

What is a trap-door one-way function?
A trap-door one-way function is easy to calculate in one direction and infeasible in the other direction unless certain additional information is known. With the addition information, the inverse can be calculated.

Exercise 4.

a. p=3; q=11, e=7; M=5
→ Encrypt:
- m = p * q = 3 * 11 = 33
- n = (p - 1) * (q - 1) = (3 - 1) * (11 - 1) = 20
- e = 7 (20 and 7 are relatively prime)
- d = 3 (verify, that (d * e) mod n = 1)

cipher-text = (plain-text ^ e) mod m = (5 ^ 7) mod 33 = 14
→ Decrypt:
plain-text = (cipher-text ^ d) mod m = (14 ^ 3) mod 33 = 5
b. p=5;q=11,e=3;M=9
→ Encrypt:
- m = p * q = 5 * 11 = 55
- n = (p - 1) * (q - 1) = (5 - 1) * (11 - 1) = 40
- e = 3 (40 and 3 are relatively prime)
- d = 27 (verify, that (d * e) mod n = 1)

cipher-text = (plain-text ^ e) mod m = (9 ^ 3) mod 55 = 14
→ Decrypt:
plain-text = (cipher-text ^ d) mod m = (14 ^ 27) mod 55 = 9

c. p=7;q=11,e=17;M=8
→ Encrypt:
- m = p * q = 7 * 11 = 77
- n = (p - 1) * (q - 1) = (7 - 1) * (11 - 1) = 60
- e = 17 (60 and 17 are relatively prime)
- d = 53 (verify, that (d * e) mod n = 1)

cipher-text = (plain-text ^ e) mod m = (8 ^ 17) mod 77 = 57
→ Decrypt:
plain-text = (cipher-text ^ d) mod m = (57 ^ 53) mod 77 = 8
d. p=11;q=13,e=11;M=7
- m = p * q = 11 * 13 = 143
- n = (p - 1) * (q - 1) = (11 - 1) * (13 - 1) = 120
- e = 11 (11 and 120 are relatively prime)
- d = 11 (verify, that (d * e) mod n = 1)

cipher-text = (plain-text ^ e) mod m = (7 ^ 11) mod 143 = 106
→ Decrypt:
plain-text = (cipher-text ^ d) mod m = (106 ^ 11) mod 143 = 7
e. p=17;q=31,e=7;M=2
- m = p * q = 17 * 31 = 527
- n = (p - 1) * (q - 1) = (17 - 1) * (31 - 1) = 480
- e = 7 (7 and 160 are relatively prime)
- d = 343 (verify, that (d * e) mod n = 1)

cipher-text = (plain-text ^ e) mod m = (2 ^ 7) mod 527 = 128
→ Decrypt:
plain-text = (cipher-text ^ d) mod m = (128 ^ 343) mod 527 = 2

Exercise 5.

Follow to example exercise above, we let:
e = 5, m = 35, C = 10
Because p and q are relatively prime, we let:
- q = 5, q = 7
- n = (p -1) * (q - 1) = (5 -1) * (7 - 1) = 24
- d = 5 (verify, that (d * e) mod n = 1)
plain-text = (cipher-text ^ d) mod m = (10 ^ 5) mod 35 = 5.

Exercise 6.

Follow to example exercise above, we let:
e = 31, m = 3599
- m = p*q
Because p and q are relatively prime, we let: q = 59, q = 61 => n = (q - 1) * (p - 1) = 3420
- We have (d * e) mod n = 1 or (d * 31) mod 3420 = 1
After using Extended Euclidean algorithm, we find that the multiplicative inverse of 31 modulo 3430 is 3031.