COMP2190 – Semester 1 2020/2021

Tutorial 7

Problems

1. What are the differences between message confidentiality and message integrity? Can you have confidentiality without integrity? Can you have integrity without confidentiality? Justify your answer.
2. Consider an 8-bit block cipher. How many possible input blocks does this cipher have? How many possible mappings are there? If we view each mapping as a key, then how many possible keys does this cipher have?
3. Suppose N people want to communicate with each of $N-1$ other people using symmetric key encryption. All communication between any two people, i and j, is visible to all other people in this group of N, and no other person in this group should be able to decode their communication. How many keys are required in the system as a whole? Now suppose that public key encryption is used. How many keys are required in this case?
4. Consider RSA with $p = 5$ and $q = 11$.
    a. What are n and $\varphi(n)$?
    b. Let $e = 3$. Why is this an acceptable choice for e?
    c. Find d such that $de = 1 \pmod{\varphi(n)}$ and $d < 160$.
    d. Can you encrypt the message $m = 57$ using the key (n, e)?
    e. Encrypt the message $m = 8$ using the key (n, e). Let c denote the corresponding cipher text. Show all work.
5. In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 7, n = 323$. What is the plaintext M?
6. In an RSA system, the public key of a given user is $e = 31, n = 4087$. What is the private key of this user?

Extended Euclidean Algorithm

```
Extended_Euclid(m,n)
```

$(A_1, A_2, A_3) \leftarrow (1, 0, m)$
$(B_1, B_2, B_3) \leftarrow (0, 1, n)$
while true do
  if $B_3 == 0$ then return A_3 //No inverse
  if $B_3 == 1$ then return B_2 //$B_2 = n^{-1} \bmod m$
  $Q = \lfloor A_3 / B_3 \rfloor$
  $(T_1, T_2, T_3) \leftarrow (A_1 - Q \times B_1, A_2 - Q \times B_2, A_3 - Q \times B_3)$
  $(A_1, A_2, A_3) \leftarrow (B_1, B_2, B_3)$
  $(B_1, B_2, B_3) \leftarrow (T_1, T_2, T_3)$

Acknowledgment

Problems 1—4 come from “Computer Networking: A Top-Down Approach,” 7/E by J. F. Kurose and K. W. Ross.