COMP90043: Cryptography and security

Week 6: RSA Signatures and Hash Functions

1. **Assume that Alice chooses two primes 43 and 47 to construct her RSA key prime factors. Help her to set up public and private keys and demonstrate encryption and decryption with an example. Choose the smallest possible non trivial exponent for the public key.**

2. **[Try at home before coming to workshop] Perform encryption and decryption using the RSA algorithm, as in Figure 9.5, for the following:**
   a. ***p* = 3; *q* = 11, *e* = 7; *M* = 5**
   b. ***p* = 5; *q* = 11, *e* = 3; *M* = 9**
   c. ***p* = 7; *q* = 11, *e* = 17; *M* = 8**
   d. ***p* = 11; *q* = 13, *e* = 11; *M* = 7**
   e. ***p* = 17; *q* = 31, *e* = 7; *M* = 2 h**

3. **Demonstrate CCA attack on textbook RSA with an example :**

   Consider n = 91, e =7 and d=31.

   M= 5; C = M^e mod n = --------

   Decrypt C without using d:

   X = (C * 2^e) mod n

   Compute 2^7 mod 91 = ------ mod 91 = ------------

   X = ---------------------

   In CCA attack, Adversary is able to get decryption of X:

   Compute Y = X^d mod n; = ----------^ (31) mod 91 = -----------

   But note that X^d == (2M) mod N = Y =

   M = (Inverse(2)* Y;

   Inverse (2) mod n = -------------

   M = ---------------* Y = ------------------

4. **Suppose we have a set of blocks encoded with the RSA algorithm and we don’t have the private key. Assume n = pq, e is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way?**

5. **What are the advantages using Hash functions in digital signatures?**

6. **Explain how you can use RSA encryption function to construct a digital signature scheme.**

7. **What characteristics are needed in a secure hash function?**

8. **What is the difference between weak and strong collision resistance?**

9. **Is it possible to use a hash function to construct a DES like block cipher? How is it possible?**

10. **Explain the birthday paradox in simple words? What is the main implication of this for hash function?**

11. **Name three important hash functions used in practice.**

12. **Discuss how the security of the hash functions depends on the length of the hash.**

13. **Why CRC checksum cannot be used as a secure hash function?**

14. **Consider the following questions in regards to Timing Attacks:**

    a. **What is a Timing Attack?**

    b. **How can Timing Attacks be prevented?**

15. **With RSA, discuss how the concept of Blinding can be implemented?**