**CSS337: Secure Systems**

**Assignment 2: Cryptography**

1. In this problem, we will compare the security services that are provided by Digital Signatures (DS) and Message Authentication Codes (MAC).

* We assume that Oscar is able to observe all messages send from Alice to Bob and vice versa.
* Oscar has no knowledge of any keys but the public one in case of DS.
* State whether and how (i) DS and (ii) MAC protect against each attack:
  + The value auth(x) is computed with a DS or a MAC algorithm, respectively.
    - ***Message Integrity***: Alice sends a message x “Transfer $1000 to Mark” in the clear and also sends auth(x) to Bob. Oscar intercepts the message and replaces “Mark” with “Oscar”. Will Bob detect this?
      * (i): auth(x) =
    - ***Replay***: Alice sends a message x “Transfer $1000 to Oscar” in the clear and also sends auth(x) to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?
    - ***Sender Authentication with cheating third party***: Oscar claims that he sent some message x with a valid auth(x) to Bob, but Alice claims the same. Can Bob clear the question in either case?
    - ***Authentication with Bob cheating***: Bob claims that he received a message x with a valid signature auth(x) from Alice (e.g., “Transfer $1000 from Alice to Bob”) but Alice claims she has never sent it. Can Alice clear this question in either case?

1. Perform encryption and decryption using the RSA algorithm (Figure 3.10) for the following:
   * p = 3; q = 11; e = 7; M =5; ***d = 3; C = 14;***
     + first, define n and Ø(n)
       - n = p\*q -> 3\*11 = 33 -> n = 33
       - Ø(n) = ((p - 1)\*(q - 1)) -> ((3-1)\*(11-1)) = 2\*10 = 20 -> Ø(n) = 20
     + Verify e, then define d:
       - given e = 7; confirming: gcd(Ø(n),e) -> gcd(20,7) = 6 -> gcd(7,6) = 1;
       - find d: (e\*d)mod(Ø(n)) ?= 1; (7\*d)mod(120) = 1; 0 < d < 20
         * 7\*1(mod 20) = 7; 7\*2(mod 20) = 22; 7\*3(mod 20) = 1;
         * d = 3
     + Given M, derive C:
       - given M = 5; Encrypt M:
         * C = M^e(mod n); C = 5^7(mod 33) -> (5^3(mod 33)\*5^3(mod 33)\*5)(mod 33) = (2\*3\*125(mod 33)))(mod 33); note: 125(mod 33) = 26; so -> (3\*52)(mod 33) = (3\*19)(mod 33) = 57 mod 33 = 14
         * -> C = 14;
     + Thus, decrypting C back into M becomes:
       - M = C^d(mod n); M = 14^3(mod 33) -> (14\*196 mod 33)(mod 33) = (14\*31)(mod 33) = 434 mod 33 = 5;
       - Thus, M = C^d(mod n) = 14^3( mod 33) = 5 = M;
   * p= 11; q = 13; e= 11; M= 7;***d = 11; C = 106;***
     + first, define n and Ø(n)
       - n = p\*q -> 11\*13 = 143 -> n = 143
       - Ø(n) = ((p - 1)\*(q - 1)) -> ((11-1)\*(13-1)) = 10\*12 = 120 -> Ø(n) = 120
     + Verify e, then define d:
       - given e = 11; confirming: gcd(Ø(n),e) -> gcd(120,11) = 10 -> gcd(11,10) = 1;
       - find d: (e\*d)mod(Ø(n)) ?= 1; (11\*d)mod(120) = 1; 0 < d < 120
         * 11\*1(mod 120) = 11; 11\*2(mod 120) = 22;...; 11\*11(mod 120) = 1;
         * d = 11
     + Given M, derive C:
       - given M = 7; Encrypt M:
         * C = M^e(mod n); C = 7^11(mod 143) = 106; used a calculator this time :P
         * -> C = 106;
     + Thus, decrypting C back into M becomes:
       - M = C^d(mod n) = 106^11(mod 143) = 7 = M
   * p= 17; q = 31; e = 7; M =2;***d = 343; C = 128;***
     + first, define n and Ø(n)
       - n = p\*q -> 17\*31 = 527 -> n = 527
       - Ø(n) = ((p - 1)\*(q - 1)) -> ((17-1)\*(31-1)) = 16\*30 = 480 -> Ø(n) = 480
     + Verify e, then define d:
       - given e = 7; confirming: gcd(Ø(n),e) -> gcd(480,7)=4 -> gcd(7,4)=3 -> gcd(4,3)=1;
       - find d: (e\*d)-1mod(Ø(n)) = 0 ; d = e^(-1)(mod 480); 0 < d < 480
         * 7\*1(mod 480) = 7; 7\*2(mod 480) = 14;...; 7\*343(mod 480) = 1;
         * d = 343
     + Given M, derive C:
       - given M = 2; Encrypt M:
         * C = M^e(mod n); C = 2^7(mod 527) = C; 2^7 = 128; 128 mod 527 = 128
         * -> C = 128;
     + Thus, decrypting C back into M becomes:
       - M = C^d(mod n) = 128^343(mod 527);
         * Note that 343 factors into 1, 7, 49, and 343 -> 1, 7, 7\*7, 7\*7\*7
         * Note that 128 can be expressed as 128 -> 2^7
         * Note that 128^343 == (((2^7)^7)^7)^7
       - -> (((2^7)^7)^7(mod 527) -> 128^7 mod 527 = 512; 512^7 mod 527 = 349; 349^7 mod 527 = 2
       - Thus, M = C^d(mod n) -> ((128^7 mod 527)^7 mod 527)^7 mod 527 = 2 = M
2. In a public‐key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M?

* M = C^d(mod n) - > M = 10^d(mod 35);
* C = M^e(mod n) -> 10 = M^5(mod 35);
* d = e^-1 mod Ø(n) -> d = .2 mod Ø(35);
* n = p\*q;
  + Find the prime factors of 35.
    - Factors of 35: 1, 5, 7, 35. Prime factors are 5 and 7;
    - let p = 5; q = 7
    - Ø(35) = (q-1)(p-1) = 4\*6 = 24
* solving for d:
  + (5\*d)mod 24 =? 1;
    - 5\*1 mod 24 = 5; 5\*2 mod 24 = 10; 5\*5 mod 24 = 1;
    - -> d = 5;
* solving for M = C^d(mod n) -> 10^5(mod 35) = 100,000 mod 35 = 5
  + -> M = 5;

1. In an RSA system, the public key of a given user is e = 31, n = 3599.What is the private key of this user?

* find d, given e = 31; and n = 3599;
  + Ø(3599) = (q-1)(p-1);
    - first identify the factors of 3599 -> 1, 59, 61, 3599
      * Now find the paired prime factors of 3599 -> 59 & 61
      * let p = 59; and let q = 61;
    - thus: Ø(3599) = (q-1)(p-1) -> (59-1)(61-1) = 58\*60 = 3480 = Ø(n)
  + Now, find d
    - -> (d\*e)(mod Ø(n)) -> (d\*31)(mod 3480) =? 1
      * (31\*1)mod 3480 = 31; (31\*113)mod 3480 = 23; (31\*226)mod 3480 = 46;

1. Consider a Diffie‐Hellman scheme with a common prime q = 11 and a primitive root α = 2.
   * If user A has public key YA = 9, what is A’s private key XA?
   * If user B has public key YB = 3, what is the shared secret key K?