Solver: Aryani Paramita

Email Address: ar0003ta@e.ntu.edu.sg

1. (a) $x^8 + x^4 + x^3 + x + 1$ in bitwise is (1 0001 1011)

   If $c_7 = 0$ → multiplication by 2 is computed as 1-bit left shift as we have bit-string lesser than $x^8 + x^4 + x^3 + x + 1$

   If $c_7 = 1$ → a modulo operation to $x^8 + x^4 + x^3 + x + 1$ must be performed after 1-bit left shift. In this case, we shall convert 2 to polynomial GF(2^8) → x

   $x.f(x) = b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x + (x^4 + x^3 + x + 1)$.

   Therefore after the shift left is performed, bitwise XOR with 00011011 which represent $(x^4 + x^3 + x + 1)$ should be performed.

   Remarks : Please refer to Section 4.6 Cryptography and Network Security by William Stallings

   (b) 5001 = 3 * 1667. Therefore we are 100% sure 5001 is a composite number

2. (a) 1 = 14 * 24 – 5 * 67

   With bezout identity, 14^{-1} mod 67 = 24.

   (b)

   (i) No fixed point S(a)==a AND no opposite fixed point S(a)== ā (bitwise complement of a)

   (ii) Non-repudiation, Authentication, Verification.

   (iii) ECC Equation : y2 mod p = (x3 + ax + b) mod 23

   In this scenario : y2 mod 23 = x3 + 9x + 17 mod 23

   Substitute (5,4) = x3 + 9x + 17 mod 23 = 3 || y2 mod 23 = 16

   Since the result of left and right hand side is not the same, (5,4) is not in E23 (9,17).

3. (a)
   - CAs has been compromised and leading to stolen certificates
   - The person whom the certificate is issued left an organization.

   (b) Attacker could generate message with M' = M || M xor Mac(K,M)

   Hash value of M' is equals to

   O1 = Mac(K,M)

   O2 = E(K, Mac (K,M) xor (M xor Mac(K,M))) = E(K,M) = Mac(K,M)

   Mac(K,M') =E(K,M') = Mac(K,M) xor Mac(K,M)= 000000...00000 (64 bit)

   Thus one can send M' and Mac of M'

   Which is different from M and without knowing Mac key K

   (c) Take I = 7 and j = 5.

   With the existensial forgery formula in lecture notes:

   $r = 2^7 17^5$ mod 36 = 13

   $s = 13 .5^{-1}$ mod 36 = 19

   x = 19 .7 mod 36 = 25

   To prove that this number would pass the verification:

   α^{si} mod 37 = $2^{19.7}$ mod 37 = 20 ===

   α^x mod 37 = 2^{25} mod 37 = 20

4. (a)

(i) First of all, attacker should obtain s' = $h(k_2, N_B)$ and message in step 2 : M' = (B,A,N_B), $h(k_1,(B,A,N_B))$. Now A will send another message to I(B):

A → I (B) : A

I(B) → A : M'

A → I(B) : (A, N_B) , $h(k_1, (A,N_B))$

A will be convinced that she is talking to B, yet she is talking to the intruder. This happens because there is no scheme to verify that the message in step 2 is fresh.

(ii) A → B : A, N_A where N_A is a nonce generated by A

B→ A : (B,A,N_A,N_B) , $h(k_1, (B,A,N_A,N_B))$

In this way, A will not be vunerable for reply attack as she can verify the freshness of N_A sent by B.

(b)

- Confidentiality: encryption of SSL payloads, using a shared secret key defined by the handshake protocol
- Message integrity: Message authentication, using a shared MAC key also defined by the handshake protocol

For reporting of errors and errata, please visit pypdiscuss.appspot.com

Thank you and all the best for your exams! ☺