Quiz 02

CMSC626

Feb 27, 2023

# Name: UMBC Id:

# Quiz Question 1

# In a public key system using RSA, you intercept ciphertext C=10 sent to a user whose public key is e=5, n=35. What is the plaintext M? Show your computation.

# Quiz Question 2

Consider a MAC scheme with encryption for 2 two message blocks B1 and B2, with its secure hash has defined as E(B1, B2) = E (E(B1) ⊕ B2). Your friend says that this hash function is not weak collision resistant and chooses two blocks C1, and C2 in the following way. It chooses some random block C1, and compute C2 as C2 =E(C1) ⊕E(B1) ⊕ B2. Prove or disprove your friend’s claim.

# Quiz Question 3

# Following code fragments show a sequence of virus instructions and its metamorphic version of the virus. Describe the effect of metamorphic code.

|  |  |
| --- | --- |
| Original code  Mov eax, 5  Add eax, ebx  Call [eax] | Metamorphic code  Mov eax, 5  Push ebx  Pop ebx  Add eax, ebx  Swap ebx, eax  Swap eax, ebx  Call [eax] |

# Answers

# Q1 Ans

n = 35, on factorization, n=5\*7, thus p=5, q=7

Thus, φ(n)=(p-1)\*(q-1)

= 4\*6 = 24

Given that e=5, then finding d such that e.d=1 mod φ(n)

Thus d=5, since 5\*5 mod 24 = 1

Thus M = Cd mod 35 = 105 mod 35

=100000 mod 35 = 5

Thus, plaintext is M=5

# Q2 Ans

Compute E(C1, C2) = E (E(C1) ⊕ C2)

= E (E(C1) ⊕ E(C1) ⊕E(B1) ⊕ B2)

= E (E(B1) ⊕ B2)

= E(B1, B2)

Thus, this function is weak collision resistant

# Q3 Ans

This code is metamorphic to original code.

The new code is extra instruction which are redundant such as push ebx and pop ebx, which basically does nothing.

Similarly, using swap twice with same registers again does nothing.

Hence new code has same behaviour as the original code.