Crypto Engineering Midterm Exam

April, 2023

Student Name : 范恩宇

Student ID : 109550135

Department : 資訊工程學系

**Question 1 :**

Answer :

Secret message = “The secret message is : When using a stream cipher, never use the key more than once” . Through “109550135\_q1.py”.

Question 2 :

Answer :

One time pad encryption of “attack at dusk” = 0x9e1c5f70a65ac519458e7f13b33 . Through “109550135\_q2.py” .

Question 3 :

Answer :

(C),(E),(G),(H) . As the diagram , key 25 is on the right of key 0 , making it possible for us to include all elements under key 1 safely . Similiarly , we can include 6 and 11 , with the same logic (but different parent) . For the remaining leaves , 26 is the only one we need to include .

Question 4 :

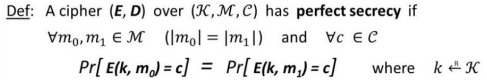
Answer :

(C) . Because the key should be encrypted under one key for each node on the path from the root to the revoked leaf , and there are log2n nodes on the path , leading to the result .

Question 5 :

Answer :

1. Set 2 encryption keys “a” and ”b” in 𝑍𝑝\* , with the property : m\*a mod p = c = m\*b mod c . We know that every element 𝑥 in 𝑍𝑝\* has an inverse 𝑥−1 ∈ 𝑍𝑝\* such that 𝑥 𝑥−1 =1 mod p and a , b ∈ 𝑍𝑝\* , so “a” must be equal to “b” , which means that P(E(k1, m) = c) = P(E(k2, m) = c) , prove that this cipher provides perfect secrecy
2. Definition of perfect secrecy is :



For OTP , E(k, m) = c = k XOR m → c XOR m = k XOR m XOR m

= k , k=1 , which is one-to-one . Thus , we can prove that OTP is perfect secrecy.

In addition , the ciphertext produced is random and equally likely to be any possible message of the same length , even if an attacker has some knowledge of the plaintext or ciphertext , this provides semantic secrecy .

1. No . OTP’s key is generated by random number generator and used only once and then discarded , leading to no statistic relation between plaintext and ciphertext
2. No , public-key encryption schemes don’t provide perfect secrecy , which can only be realized by symmetric key encryption like OTP . Although public-key encryption provides semantic security , its security depends on the complexity of mathematical problems , for example : A quantum computer can break the security easily . In addition , public-key encryption can also be vulnerable to attacks like chosen ciphertext attacks or side-channel attacks , which may reveal private key or plaintext . Above all makes public-key encryption can’t provide perfect secrecy .

Question 6 :

Answer :

1. First turn the formula given to relation x2-x1 = a(x1-x0)(mod p) , we can get (assume that x1-x0 and m are relatively prime) a = (x2-x1)( x1-x0) mod p where division is mod m (using extended Euclidean algorithm ) . The increment b ’ll be given by b = (x1-ax0) mod p , so we found the formula and may predict the rest of the sequence.
2. This means that using congruential generator as the keystream generator for a stream cipher would not be secure , because an attacker could easily predict the rest of the sequence through small amount of information .
3. Since the attacker knows all the parameters needed for the formula , he/she can infer the complete sequence .
4. By Question 6-1, we proved that if we know a&b in the given relation , we can infer the full result , while a&b can be inferred once we have 3 successive value xn-1~n+1 . Thus , an attacker only needs to know 3 successive outputs to predict the complete sequence.

Question 7 :

Answer :

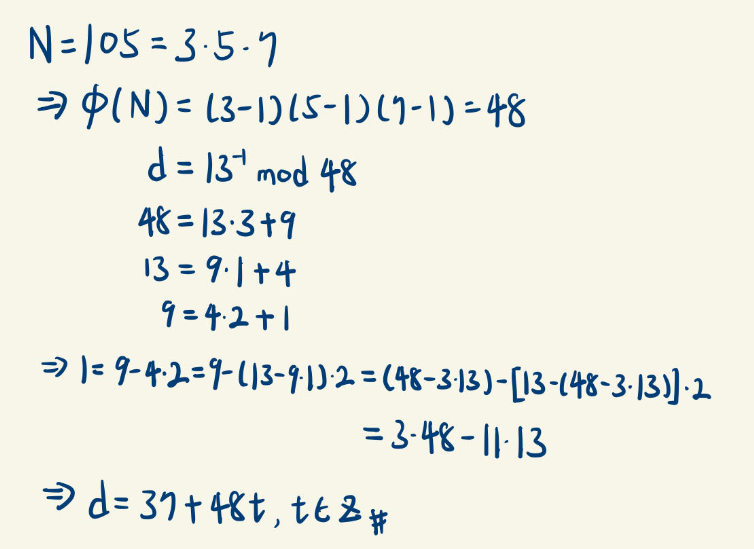
(D) . When N is a product of three distinct primes, we can make φ(N) = φ(pqr) = φ(p)φ(q)φ(r) where p, q, and r are three distinct prime numbers .

Since φ(n) is the Euler totient function , for the three distinct prime numbers p, q, and r, we have: φ(p) = p - 1 (p is prime, all positive integers less than p are relatively prime to p , except for the multiples of p, which are exactly (p-1) numbers) . Similarly, φ(q) = q - 1 and φ(r) = r – 1 .

Former result makes φ(N) = φ(p)φ(q)φ(r) = (p-1)(q-1)(r-1) .

Question 8 :

Answer :



Question 9 :

Answer :

Ciphertext = “20814804c1767293bd9f1d9cab3bc3

e7ac1e37bfb15599e5f40eef805488281d” . Through “109550135\_q9.py”.

Question 10 :

Answer :

(A),(C) . From given assumption , we can know that f(gx, gy) = gxy  is also difficult to compute , making f(gx, gy) = g2xy and f(gx, gy) = √gxy are also difficult to compute , since they are just the square and root of the original formula .