2024NetSec_CryptoSummative1_Answers

Jiayang Xu

1.

Round	Subkey
1	60B7405C2443C26C54B7B623F685A10F
2	F585361ED1C6F4728571425173F4E35E

2. A penguin as below:

3. An encryption system that satisfies IND-CPA ensures that even with multiple chosen plaintexts, the ciphertexts reveal no useful information about the original data. Machine learning models rely on patterns in data, but IND-CPA encryption hides such patterns, preventing the model from learning anything useful to break the encryption.

4. 45947425

5.

String	Hash
1100001101010000	101010000
1100001101000001	101010000

6. a.

   Modulus=B86DF078C3301C0FDBE142E2D721039DD6CAE4428E5D50EF2504A5549F8CA6A10BFE9FD56877FE8CFF4886556935C1149D3E699C3085EB4990979A064997E7CCF284195633B82D25C7F9BDD1F128FE72E8A5C8B75C63E3935A433E5592A1EB735EB04678AA9FE44AE1987D4C88156C5C0CB7A2C8C86782DA3EE2E082A63E20F2D5F88A1C2E9E10D67DC0B120E4C6D5814149C108EFA384F5D1DE4ABAD59DED63C21AFCB3F5B03AF043515FC5C135405712511D07EB37547F603CA7F62063330CE772F4DC07E5D8DE196449C668EA57FA9092488D2FA72B9F6FA8455D71D4381116C5C8F18F9F7EFA9C922067BA8D4A6A1C03A740E880FEEEA06849CC56B959B

   b.

Student id	Decrypted result of cipher9543.txt
2829543	710495eccab323cf

7. If

$$c_2 = m_0 \cdot H_1(H_2(m_0)/c_3) \bmod n$$

then

$$b = 0$$

else if

$$c_2 = m_1 \cdot H_1(H_2(m_1)/c_3) \bmod n$$

then

$$b = 1$$

Therefore, BadModPKC is not IND-CPA secure.