Contents

[Task 1 2](#_Toc31957228)

[Task 2 3](#_Toc31957229)

[Task 3 3](#_Toc31957230)

[References 4](#_Toc31957231)

**Cryptographic Concepts – Assignment 2 – Part 2**

# Task 1

Actually, I agree with the design proposed by Jerry because we know that adding more complexity directly increases the security (Blake, Seroussi & Smart, 2005) . Also, the design proposed by Tom is for public which can be cracked in less time and efforts whereas the design proposed by jerry will consume more time and efforts than tom due to its complexity. Also, the process of cracking jerry’s design probably need more steps and knowledge.

Let’s consider an example, assume that Ek(M) = C is encrypted format for the message M and the decrypted plaintext format would be Dk(C) = M and as per tom’s design public can retrieve the plaintext ***m*** or ***K***, the secret key with the help of ciphertext *C*. So for, C= (Ek(m)⊕m)||Ek(m)⊕1111…11) then Ca = Ek(m)⊕m, Cb= Ek(m)⊕1111…11 C = cb⊕1111…11 then ends with m =ca⊕c′

Though the design proposed by Jerry is better than Tom it still crackable but need more steps and time

# Task 2

There are ways to available to reduce the number of keys. Firstly, we can implement RSA cryptosystem model which can help to achieve confidentiality and as well as integrity (Margaret, 2018) . Also, using RSA crypto system involves the requirements of complex mathematics which increase its complexity and making it harder to crack.

In this method each user will be assigned with 2 keys one is public key and another one is private key. Assume that Alice sending message to Bob by encrypting with Bob’s public key so when Bob receive the message he can decrypt with his private key.

The RSA formula for this scenario would be Nk = n\*2 = 100\*2 = 200.

So Nk = 200

# Task 3

In general except for the S boxes the DES components are linear. As per this the input in X- boxes will be identical regardless of whether it starts from *P* and *K* or *P* and *K.* So here the X given is the bit by bit enhance of X.

As per the DES encryption the P should be divided into 2 equal portions so we name them as L0 and R0 (Assuming L represents Left hand side and R represents right hand side).

Now the equation would be [L0][R0] K → [R0][L0 ⊕ f(R0, K)].

Now considering K, C, P are identical and divide P into 2 equal portions namely L0 and R0. So the formula would be [L0][R0] → [R0][L0 ⊕ f(R0, K)] so the values for R, K, and L would be R0 = R0 ⊕ 111 . . . L0 = L0 ⊕ 111 . . . K = K ⊕ 111.

So when we combine all the functions into one ,

[L0][R0] → [R0 [L0 ⊕ f(R0, K)]

= [L1] [R1]

= C

In this the L0 derived from R0

# References

Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal Of Cryptology*, *4*(1). doi: 10.1007/bf00630563

Blake, I., Seroussi, G., & Smart, N. (2005). *Advances in Elliptic Curve Cryptography*. Cambridge: Cambridge University Press.

Margaret, R. (2018). What is RSA algorithm (Rivest-Shamir-Adleman)? - Definition from WhatIs.com. Retrieved 7 February 2020, from <https://searchsecurity.techtarget.com/definition/RSA>