Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Class Test 1
Subject – Cryptography and Network Security (CS60041)
Full Marks – 30 Date: 15.09.2023 Time: 9 AM to 10 AM

Answer all the questions

1. We know that DES is a 64-bit plaintext block cipher which uses a 56-bit key. Now, we try to transform DES into a block cipher with 128-bit plaintext, that we denote XDES. We use a 112-bit key which is split into two DES keys K1 and k2. For this, we define the encryption of a 128-bit block x as follows

- we split x into two 64-bit halves x_L and x_R such that $x = x_L \| x_R$
- we let $u_L = DES_{k1}(x_L)$ and $u_R = DES_{k1}(x_R)$
- we split $u_L \| u_R$ into four 32-bit quarters u_1, u_2, u_3, u_4 such that $u_L = u_1 \| u_2$ and $u_R = u_3 \| u_4$
- we let $v_L = DES^{-1}_{k2}(u_1 \| u_4)$ and $v_R = DES^{-1}_{k2}(u_3 \| u_2)$
- we split $v_L \| v_R$ into four 32-bit quarters v_1, v_2, v_3, v_4 such that $v_L = v_1 \| v_2$ and $v_R = v_3 \| v_4$
- we let $y_L = DES_{k1}(v_1 \| v_4)$ and $y_R = DES_{k1}(v_3 \| v_2)$
- we define $y = y_L \| y_R$ as the encryption $XDES_{k1\|k2}(x)$ of x

(a) Draw a diagram of XDES

(b) Explain how (i) XDES can work as 3DES and (ii) XDES can work as DES

(c) (i) Do you think that XDES is more secure that 3DES? (ii) Do you think that XDES is more secure that DES?

(d) Let x and x' be two plain two plaintexts, and let $y = XDES_{k1\|k2}(x)$ of x and $y' = XDES_{k1\|k2}(x')$ of x' be the corresponding known ciphertexts. Explain how a smart choice of x and x' allows us to detect that we have $u_4 = u_4'$ and $v_4 = v_4'$ simultaneously.

(e) Use the previous question i.e. as mentioned in (d), to mount a chosen plaintext attack whose goal is to find (x, x') pair with $u_4 = u_4'$ and $v_4 = v_4'$ simultaneously. What is the complexity of this attack?

(f) Explain how to use this attack in order to reduce the security of XDES to the security of DES against exhaustive search? How can you compare now about the security of XDES to the security of 3DES?

[6x5=30]