MANCHESTER 1824
The University of Manchester

Feedback on Ex3

Exercise Question – E3.1

By applying DES twice using two different 56-bit keys, K1 and K2, to encrypt a message, M, i.e. $C=E_{K2}[E_{K1}[M]]$, where C is the ciphertext, we have a double DES encryption. Would this double DES encryption scheme double the security level of a single DES scheme? Justify your answer.

Exercise Question – E3.1

- **Assuming** *n1* and *n2* are, respectively, the lengths of K_1 and K_2 and $n_1 = n_2 = n$.
- **Case 1:** without using meet-in-the-middle method, i.e. by using brute-force attack

The anticipated number of attempts before compromising the encryption is: $2^{2n}/2=2^{2n-1}$

- **Case 2:** using meet-in-the-middle method

With the Meet-in-the-Middle attack, the attacker first computes $E_{K1}(M)$ for all values of K_1 and $D_{K2}(C)$ for all possible values of K_2. He then compares the results from the two sets. If the result from any of the $E_{K1}(M)$ set matches with a result from the $D_{K2}(C)$ set, the pair of K_1 and K_2 is probably the correct keys. In this case, the anticipated number of attempts before compromising the encryption is: $2^n + 2^n=2^{n+1}$.

- As $2^{n+1} < 2^{2n-1}$ (when $n>2$), so: an attacker can use the Meet-in-the-Middle attack to attack the double DES scheme more efficiently than the brute-force attack.

Exercise Question – E3.2

The diagram given in the slides illustrates an early version of the ATM (Automatic Teller Machine) solution. From the diagram, it can be seen that:

- Cash card stores the ciphertext of the user's Identity (ID) and PIN that are encrypted using a symmetric key, $K_{card/ATM}$.
- The communication between ATM and bank backend office is secured using another symmetric key, $K_{ATM/Bank}$.

(i) Identify any vulnerability in this solution, and propose a solution to address any vulnerability that you have identified.

The vulnerability was that PIN verifications were carried out in ATMs.

In the current solution, the PIN is encrypted using a key shared with the bank backend office, i.e. ATM does not unwrap the PIN – the PIN verification is done at the backend office, not at ATM! ALSO 3DES is used to replace DES.

Exercise Question – E3.2

(i) Are there any other issues that you could identify from this application of symmetric ciphers?

Key management problem:

- either all the cards (issued by a particular vendor) and ATM machines (in this case, ATM machines would need to be vendor dependent) share the same key - once a key is compromised, then all the cards using the same key will be put at risks,
- or different cards use different keys - is this viable? How about user mobility requirement?