The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security

Week 6 Workshop – 19th and 21st April 2021

1. For Playfair cipher, estimate the unicity distance, assuming that all keys are equally likely.

2. Decipher the ciphertext AR HM CW CO KI PW, which was enciphered using Playfair cipher with the key shown below.

H A R P S
I C O D B
E F G K L
M N Q T U
V W X Y Z

3. Suppose that the keys used with DES consist only of letters A-Z (i.e. capitals only) and are 8 letters long. Give an approximation of the length of time it would take to try all such keys using exhaustive search, assuming each key can be tested in one μsec. Do the same for keys 8 letters or digits long.

4. Let X' denote the bit-by-bit complement of a block X.
a) Show that if $C = DES_K(M)$, then $C' = DES_{K'}(M')$.
b) Explain how this property can be exploited in a chosen -plaintext attack to reduce the search effort by roughly 50%.

5. (Exercise from the Text)
Show that DES decryption is the inverse of DES encryption.

6. (Exercise from the Text)
To show that the 32-bit swap after the sixteenth iteration of DES is indeed needed, first consider the following notation.

A || B	= the concatenation of the bit strings A and B
$T_i(R\|\|L)$	= the transformation defined by the i^{th} iteration of the encryption algorithm, for $1 \le i \le 16$
$TD_i(R\|\|L)$	= the transformation defined by the i^{th} iteration of the decryption algorithm, for $1 \le i \le 16$
$T_{17}(R\|\|L)$	= L||R. This transformation occurs after the sixteenth iteration of the encryption algorithm.

a) Show that the composition $TD_1(IP(IP^{-1}(T_{17}(T_{16}(L_{15}||R_{15})))))$ is equivalent to the transformation that interchanges the 32-bit halves, L_{15} and R_{15} . That is, show that

$$TD_1(IP(IP^{-1}(T_{17}(T_{16}(L_{15}||R_{15}))))) = R_{15}||L_{15}$$

b) Now suppose that we did away with the final 32-bit swap in the encryption algorithm. Then we would want the following equality to hold:

$$TD_1(IP(IP^{-1}(T_{16}(L_{15}||R_{15})))) = L_{15}||R_{15}$$

Does it?

7. What are the subkeys for the DES key of all 1's and the DES key of all 0's?

8. The following 4 DES keys are known as "weak keys". Find out why.

0101 0101 0101 0101
1F1F 1F1F 0E0E 0E0E
FEFE FEFE FEFE FEFE
E0E0 E0E0 F1F1 F1F1

9. In the previous question we have identified some "weak keys" for DES, each of which produces identical subkeys. Explain how in the case of a weak key in a chosen plaintext attack the Feistel cipher can be broken to discover the plaintext corresponding to the intercepted ciphertext.

10. In addition to 4 weak keys identified in Question 2, are there any other weak keys for DES? Prove your answer.