ELEN 330 Information Engineering Techniques
May 2005 Class Test

Instructions:

1. Answer all questions
2. Show all working: marks are awarded for all working and logical reasoning and not only the correct answer
3. Justify any assumptions made
4. This is a closed book examination. An engineering calculator and one handwritten information sheet is allowed

Question 1 **10 marks**

a) Derive the two translation tables from the following permutation functions for monoalphabetic substitution cipher:

$P_1(a) = (3 * a) \bmod 26$
$P_2(a) = (5 * a + 13) \bmod 26$

Hence double-encrypt the following plaintext using first a 5 column transposition cipher, and then by using the polyalphabetic substitution defined above. Explain the choice of padding characters you have used to fill the transposition table. **(6 marks)**

```
ALL HAIL CAESAR
```

b) What elements of encryption do the two ciphers (polyalphabetic and transposition) bring into the resultant cipher above? **(2 marks)**

c) Why is the one time pad, when used correctly, an unbreakable cipher? **(2 marks)**

Question 2 **10 marks**

a) Derive the lookup table for a four bit CRC with magic polynomial (divisor) 1010. **(6 marks)**

b) Explain fully concept of a digital signature, and how it is used in practice to sign documents. **(4 marks)**

Question 3 **10 marks**

A bank previously used ECB (Electronic Codebook Mode) together with a known secure symmetric block cipher to encrypt the data between satellite branches, ATM's and the head office where the transactions are processed overnight. However, when they used this

mode, they found that the communication was prone to block replay attacks on depositor messages. The significant portions of the message format are:

Time Stamp	Account Number	Depositor Account Number	Amount	…

Where Account Number is the number of the account the money must go to, and Depositor Account Number is the number of the account that the money must come from.

They found that the hackers held two accounts at the bank. They would initiate a transfer from one of the accounts to the other. Then they would intercept the message on the communications channel and somehow change the Depositor Account Number to that of some unsuspecting customer of the bank. The bank would then receive the message, and deposit money from the unsuspecting customer's account into the hacker's account. The hackers always withdrew the money immediately, so the deposits could not be reversed.

An analyst advised them to change to a different cipher mode to prevent replay attacks from occurring. The bank then changed to OFB (Output Feedback Mode), with a suitable Initialisation Variable (IV). However, the bank found that the problem persisted. It is assumed that the hackers know the message format, as this was never kept secret.. It is further assumed that the hackers know the account numbers of many customers and that the communications channel is insecure.

a) Explain why block replay attacks are possible under ECB mode. **(1 mark)**

b) Explain the OFB mode with the aid of a diagram. **(4 marks)**

c) Using your explanation of OFB, show how the hackers could still alter the messages in their favour. **(4 marks)**

d) The bank is also using a 1024 bit implementation of RSA. This means that each part (n,e) of the public key and (n,d) and private key is 1024 bits long. What should the size of the message and of the ciphertext blocks be in this implementation? State your answer in bits. **(1 mark)**