ELEN 330 – Information Engineering Techniques
Examination, June 2003

Instructions to candidates:

1. Answer all questions. Total marks for this paper is 75. Full marks is 65. Note that the total marks per question varies.
2. Show all working: marks will be allocated for all working and logical reasoning and not just for the correct answer.
3. Give reasons for any assumptions that are made.
4. Type 2 exam – this is a closed book exam. Candidates are allowed to use an engineering calculator and one handwritten A4 information sheet.

Question 1

The two translation tables below represent Caesar ciphers E_1 and E_2.

```
abcdefghijklmnopqrstuvwxyz
CDEFGHIJKLMNOPQRSTUVWXYZAB

abcdefghijklmnopqrstuvwxyz
PQRSTUVWXYZABCDEFGHIJKLMNO
```

(a) Using the sample plaintext

```
P = ZORK RESIDENT
```

show that $E_1(E_2(P)) = E_2(E_1(P))$ for the sample plaintext. This exercise demonstrates that monoalphabetic ciphers of this type are probably commutative, i.e. they satisfy the relation $E_1(E_2(P)) = E_2(E_1(P))$ for all plaintexts P. **(4 marks)**

(b) Write down the translation table E_3 for which $E_3 = E_1(E_2(P))$. What is the name of this property? **(3 marks)**

(c) Demonstrate using the same plaintext that for columnar transposition ciphers of column numbers 4 (E1) and 5 (E2), the cipher is not commutative and therefore that, in general, transposition ciphers are not commutative. **(4 marks)**

(d) Shamir's three pass protocol is a secure means of sending messages in a public communication channel without exchanging keys at all, and relies on the use of a commutative cipher. The information sheet summarises Shamir's protocol. Derive equations showing an implementation of the protocol using the XOR-type one-time pad and demonstrate that for this particular cipher the protocol is *not secure* if an eavesdropper is able to intercept all communications between the parties. **(7 marks)**

Question 2

(a) Residents of the planet Zork have a 39 day year. They are only slightly surprised to hear that for a given individual, 27 other Zorks have to be in the same room for a better than even chance that they share a birthday with someone else. However, they are very surprised to learn that only 8 Zorks need to be in a room for a better than even chance that any pair of them shares a birthday. Using your knowledge of probability, produce an argument (with calculations) that convinces the Zorks that both your claims are correct. **(12 marks)**

(b) The birthday paradox described in part (a) of the question is analagous to the birthday attack on hash functions. Explain the parallel between the two fully. Using a rule of thumb you know about hash functions and the birthday attack, what is the minimum length of the hash function required to resist attack from a computer system which is barely capable of performing $\mathbf{2^{70}}$ hashes in a reasonable amount of time? **(4 marks)**

(c) Hash functions are useful in the authentication process. Give two examples of how they are used in the authentication process. **(2 marks)**

Question 3

(a) The Diffie-Hellman key exchange algorithm makes it possible for two people communicating publicly to "tell" each other something that will allow them both to arrive at a secret key that no one else can deduce. The algorithm relies on the difficulty of finding logarithms in a Galois field, and is summarised in the information sheet. Extend this idea to a protocol that allows *three* people to share *the same key* in such a way that no other member of the public is able to deduce the key.

In answering this question you *must* draw a diagram showing the three parties and the information exchanged between them. Note that there are two ways of solving this problem: one is an elegant extension of the Diffie-Hellman algorithm itself and the other is a less elegant solution that makes use of the original Diffie-Hellman algorithm and a symmetric algorithm. 9 marks will be awarded for the more elegant solution, 5 marks for another. You may not use a public-key algorithm such as RSA as part of your solution.

(9 marks)

(b) Using the prime numbers 5 and 13 as a starting point, generate public and private keys for the RSA algorithm (hint: the number e=29 can be inverted by trial and error in a couple of minutes). Hence write down the encryption and decryption functions corresponding to your key choice. Use these functions to encrypt and decrypt a suitably small message, say M=2. Note: using the above keys this can be done with an ordinary calculator in about 3 minutes.

(10 marks)

Question 4

(a) The year is 2030. Powerful embedded computing technology is so inexpensive that it's virtually free. The SA mint is about to start manufacturing tough plastic coins with a variety of security features, most important of which is a passive transponder with built-in microprocessor and cryptographic engine. This electronics is to be powered by a loop antenna embedded in the circumference of the coin when it is brought close to a reader. The coin must be able to authenticate itself and its value to a coin reader when required (such as in any vending machine or even personal coin readers which people may carry). The coin factory (mint) must be able to program the coin's value at minting time and it must not be possible users to alter this value at run time (use by the public).

Using block diagrams, fully specify the cryptographic functions and keys required to implement the features described. Be sure to consider the cryptography required both at minting time as well as at run time. Be clear about what kind of attacks the coin may be subjected to, as how well your coin design is able to deal with the attacks. You may add innovative features if you wish to. **(12 marks)**

(b) Rufus is having trouble with the RSA data listed below. Determine, in each case, what the problem is. (All the symbols have their usual meaning in the context of RSA).

(i) $p = 9$ $q = 13$ $e = 17$ $M = 8$
(ii) $p = 13$ $q = 17$ $e = 9$ $M = 2$
(iii) $p = 19$ $q = 13$ $e = 11$ $M = 211$
(iv) $p = 7$ $q = 13$ $e = 11$ $M = 11$

(8 marks)

Information Sheet

Diffie-Hellman Key Exchange

Two people (call them X and Y) communicating in public are able to choose a secret key as follows: First, a large prime n and a random number between 0 and n, call it g, are agreed on. These numbers can be communicated in the clear. X randomly selects a number x that is smaller than n and divulges it to no-one. Y randomly selects a number y which is smaller than n and divulges it to no-one. X calculates $a = g^x \bmod n$ and communicates it to Y. Likewise, Y calculates $b = g^y \bmod n$ and communicates it to X. X can now compute $k = (g^x)^y \bmod n = g^{xy} \bmod n$ and Y can calculate $k = (g^y)^x \bmod n = g^{xy} \bmod n$ and they now both know the key k. No-one else is able to deduce k because only g and n are known to the public and x cannot be found in a reasonable amount of time from g^x.

Shamir's Three-pass Protocol

Using this algorithm, Bob and Alice are able to exchanges messages securely in a public communication channel without first exchanging keys. The algorithm relies on the use of a commutative cipher (note that this is a necessary but not sufficient condition for use in the protocol). Alice selects a secret key K1 which she communicates to no-one and Bob selects a secret key K2 which he communicates to no-one. Messaging occurs as follows:

1. Alice wishes to communicate plaintext P to Bob. She calculates $C_1 = E_{K1}(P)$ and sends it to Bob.
2. Bob Calculates $C_2 = E_{K2}(C_1) = E_{K2}(E_{K1}(P))$ and sends it to Alice.
3. Alice calculates $C_3 = D_{K1}(C_2) = D_{K1}(E_{K2}(E_{K1}(P))) = D_{K1}(E_{K1}(E_{K2}(P))) = E_{K2}(P)$ and sends it to Bob.
4. Bob then deciphers $C_3 = E_{K2}(P)$ with his key K2 to obtain the message P.