OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

Summer Examination 2012

CS4614: Introductory Network Security

Professor Ian Gent,
Professor J. Bowen,
Dr. S.N. Foley

Answer *all* questions

1.5 Hours

1. a) Explain the properties of a one-way hash function. (*6 marks*)

   b) Each year a lecturer encrypts the summer exam paper f as $\mathsf{rc4}(k) \oplus f$, where $\mathsf{rc4}$ is a stream cipher, k is a secret password (known only to the lecturer) and $\oplus$ is bitwise XOR. Explain how a student, given the ciphertext, might discover this year's exam paper before it has been made public. (*6 marks*)

   c) A fingerprint reader with a False Accept Rate (FAR) of 0.001 is to be used to control student access to the Computer Science Laboratories. Should the reader be used to *identify* students or to *authenticate* students? Explain your answer. (*6 marks*)

   d) You are directed to visit `https://www.ucc.ie` in your browser. Give *two* examples of why you might, unknowingly, not end up at UCC's web-site. (*6 marks*)

   e) An authentication server uses the following Java code to generate a session `key` and initialization vector (`IV`) for a client.

```
KeyGenerator kg= KeyGenerator.getInstance("DES");
kg.init(new Random(0));
SecretKey key= kg.generateKey();
byte[] IV = 0;
Cipher cipher= Cipher.getInstance("DES/ECB/PKCS5Padding");
```

   Identify and explain any security vulnerabilities in the code above. (*6 marks*)

---

2. Given suitable public generator g and modulus n, principals A and B generate suitable secrets x and y, respectively, and engage in the Diffie-Hellman Key exchange:

$$\begin{array}{lll} \text{Msg1:} & A \rightarrow B & g^x \bmod n \\ \text{Msg2:} & B \rightarrow A & g^y \bmod n \end{array}$$

   a) How do A and B determine their shared key? Why does this protocol *not* provide authentication of A or B. (*10 marks*)

   b) Suppose that A and B own RSA public keys K_A and K_B, respectively. Modify the protocol so that it provides authentication for both A and B. Further modify the protocol so that on completion A and B can be sure that they share the exchanged key with each other. Be sure to explain the role of any trusted third parties in your answer. (*15 marks*)

---

3. Alice (A) wishes to communicate securely with Bob (B) and proposes a symmetric session key K_{AB}, a copy of which she intends to give to Bob. Trent is a trusted third party who provides a message translation service. Trent shares symmetric K_{AT} with Alice, and symmetric key K_{BT} with Bob. All keys are 128-bit AES keys (CBC mode). The following protocol is used to pass the key K_{AB} to Bob.

$$\begin{array}{lll} \text{Msg1}: & A \rightarrow T: & B, \{A, K_{AB}\}_{K_{AT}} \\ \text{Msg2}: & T \rightarrow A: & \{A, K_{AB}\}_{K_{BT}} \\ \text{Msg3}: & A \rightarrow B: & \{A, K_{AB}\}_{K_{BT}} \end{array}$$

   a) Describe how this protocol might be used in practice to provide authenticated secure access to network resources. (*13 marks*)

   b) Illustrate how a third principle Eve (who shares secret key K_{ET} with Trent) can subvert the protocol to get a copy of the key K_{AB} that Alice gives to Bob. (*12 marks*)