OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

Summer Examination 2013

CS4614: Introductory Network Security

Professor I. Gent,
Professor B. O'Sullivan,
Dr. S.N. Foley

Answer *all* questions

1.5 Hours

1. a) Alice sends message M to Bob over a untrusted network. Assuming they share a secret, sketch how message secrecy, integrity and authentication should be provided. (*6 marks*)

   b) Explain how *salt* defends against a password *pre-computation dictionary attack*. (*6 marks*)

   c) In the movie *Skyfall*, James Bond's Walther PPK handgun has a biometric reader designed to recognise his palm print, so that *only* he can fire it. Explain whether the designers of this authentication mechanism need to worry about the Birthday Paradox. (*6 marks*)

   d) Alice receives a document signed by Bob and a certificate for his public key. Sketch the operations carried out by Alice to confirm the document's authenticity. (*6 marks*)

   e) If Alice and Bob know each other's public keys (K_A and K_B, respectively) and K_{AB} is a session key, then explain which of the following provide a digital signature for message M.

$$A \rightarrow B : \{M\}_{K_{AB}}, \{\{h(M), K_{AB}, A, B, \ldots\}_{K_A^{-1}}\}_{K_B} \quad (1)$$

$$A \rightarrow B : \{M, h(M)\}_{K_{AB}}, \{\{K_{AB}, A, B, \ldots\}_{K_A^{-1}}\}_{K_B} \quad (2)$$

(*6 marks*)

(*30 total marks*)

---

2. Alice A and Bob B share secret keys K_{AT} and K_{BT}, respectively, with trusted authentication server T. Alice wishes to communicate securely with Bob and initiates the following protocol.

$$\begin{aligned}
&\text{Msg1}: \quad A \rightarrow B \quad : A \\
&\text{Msg2}: \quad B \rightarrow T \quad : A, B \\
&\text{Msg3}: \quad T \rightarrow B \quad : \{K_{AB}\}_{K_{AT}}, \{B\}_{K_{AT}}, \{K_{AB}, A\}_{K_{BT}} \\
&\text{Msg4}: \quad B \rightarrow A \quad : \{K_{AB}\}_{K_{AT}}, \{B\}_{K_{AT}},
\end{aligned}$$

   a) Describe how this protocol should be used to provide authenticated secure access to network resources. Highlight how it is different to a Kerberos-style protocol. (*15 marks*)

   b) Describe an attack on the protocol whereby a malicious user Mike can trick Alice into believing that she is initiating a secure connection with Bob (but it is actually Mike). (*10 marks*)

(*25 total marks*)

Question 3 overleaf.

3. UCC lecturer Alice securely submits exam results to a network-based Exams-Office service using the Java code fragment below. Results `rslts` are sent over a socket-based connection (encapsulated as `DataOutputStream out`). Alice's Java KeyStore `keystore` stores her public DSA key, alias `"alicePK"`.

```
Random rangen = new Random(0);
byte[] keySession = new byte[2];
rangen.nextBytes(keySession);
SecretKeyFactory desF = SecretKeyFactory.getInstance ("DES");
KeySpec ks = new DESKeySpec(keySession);
SecretKey key = desF.generateSecret(ks)
Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
cipher.init(Cipher.ENCRYPT_MODE,key);
byte[] cBytes= cipher.doFinal(rslts)
out.write(cBytes);

String alice= "alicePassword".toCharArray();
PrivateKey priv = (PrivateKey) keystore.getKey("alicePK",alice);
Signature signature = Signature.getInstance ("DSA");
signature.initSign(priv);
byte[] sig = signature.sign(keySession);
out.write(sig);
```

a) Identify and explain the security vulnerabilities in this implementation. (*15 marks*)

b) It has been suggested that it would be better to use Java SSL to secure the connection between Alice and Bob. Outline how Java SSL should be used in this case and include an explanation of how the use of public key certificates in the protocol can help Bob to discover Alice's public key. (*10 marks*)

(*25 total marks*)
