Computer Security
Coursework Exercise CW1

Cryptography and Protocols

School of Informatics
University of Edinburgh
http://www.inf.ed.ac.uk/teaching/courses/cs

This is an individual assessed coursework exercise. It will be awarded a mark out of 25. It is one of two assessed exercises in the Computer Security course. Each exercise is worth 12.5% of the final result for the course. The deadline for completing this coursework is 16:00, 16th March 2015. The final page summarises submission instructions. This exercise explores some topics in cryptography and protocols. This answers should be submitted on paper, by hand at the ITO. To answer the questions you will need to consult the lecture slides and additional resources such as the referenced papers that are cited in the lecture slides.

Question 1 The following questions are intended to help you further understand some of the concepts learned in the lectures regarding the use of pseudo-random number generators, and key entropy.

(a) A bit source S produces a statistically biased random sequence of bits $b_1b_2b_3\ldots$ and it is known that for each bit b_i, $\mathit{prob}(b_i = 0) = p$ and $\mathit{prob}(b_i = 1) = (1 - p)$, for some $0 < p < 1$ where $p \neq 1/2$. Devise a simple algorithm to extract from S an unbiased random bit sequence $a_1a_2a_3\ldots$ (i.e., produce a bit sequence such that $\mathit{prob}(a_i = 0) = \mathit{prob}(a_i = 1) = 1/2$). Justify that your algorithm works as required.

(b) A colleague is preparing a presentation in which he wants to demonstrate the superiority of the public key cryptosystem RSA over the conventional cryptosystem AES. One of his arguments is that because RSA uses a key size of 2048 bits, while AES uses a key size of 128 bits, RSA offers a more secure alternative (because 2048 is a much larger number than 128). Do you agree with this argument? Why or why not?

(c) A vendor is attempting to sell cryptographic software to your company and suggests that their software uses a key length of 160 bits, and hence requires $O(2^{160})$ operations to attack the cipher. The vendor explains that these 160 bits are derived as follows: the software repeatedly selects 20 random characters from the set $\{a, \ldots, z\}$ and that since 8 bits are used to encode each character, the key length is $8 \times 20 = 160$ bits long. Do you believe his claim that this cipher offers 160 bits of security through its key? Why or why not?

Question 2 Attack on variants of raw RSA.

(a) Assume that Alice wants to keep her RSA modulus N secret to everybody except to Bob. Alice uses $e = 3$ as public exponent. To encrypt a message m, Bob computes $c = m^3 \bmod N$ and sends c to Alice. Assume that Eve gets $c_1 = m_1^3 \bmod N$ and $c_2 = m_2^3 \bmod N$ and already knows m_1 and m_2; explain how Eve can recover N.

(b) Assume that Alice and Bob want to share the same modulus N but use different public exponent. Alice uses $e_A = 3$ and Bob uses $e_B = 5$. Let d_A and d_B be the corresponding private exponents. Explain how Alice can recover d_B from d_A.

(c) Assume that Alice and Bob want to share the same modulus N but use different public exponent. Alice uses $e_A = 3$ and Bob uses $e_B = 5$. Now Charlie wants to encrypt a message m for Alice and Bob. He sends:

$$c_A = m^3 \bmod N$$

to Alice and

$$c_B = m^5 \bmod N$$

to Bob. Explain how Eve can recover m from N, c_A and c_B.

Question 3 Alice and Bob believe they share an k-bit secret key, and want to confirm that they do agree on the the same key. In order to achieve this over an insecure channel, while preventing an attacker from learning the secret key, they execute the following protocol. Let k_A be the key held by Alice, and k_B the key held by Bob.

1. Alice generates a random k-bit value r.
2. Alice computes $x = k_A \oplus r$, and sends x to Bob.
3. Bob computes $y = k_B \oplus x$ and sends y to Alice.
4. Alice compares r and y. $Ifr = y$, then she knows $k_A = k_B$ that is, she and Bob do agree on the same secret key.

(a) Show how an attacker can learn the shared secret key.

(b) Show how an attacker can make Alice and Bob believe they do not share the same key.

Question 4 In class, we saw the Diffie-Hellman protocol, which is a two-party key establishment protocol secure against passive attackers. However, as we saw, the Diffie-Hellman protocol is insecure against active attackers. Indeed, a malicious agent can mount a man-in-the-middle attack to learn a key not intended for him. This attack is possible because their is no mechanism to authenticate the two parties to one another. We consider the following extension of the Diffie-Hellman protocol to thwart this attack. We assume that the parties A and B have a private signing key sk_A and sk_B respectively, and a certificate on the corresponding public key CERT_A and CERT_B respectively.

$$\begin{array}{ccc} A & & B \\ & \xrightarrow{\qquad g^x \qquad} & \\ & \xleftarrow{g^y,\ B,\ \mathsf{CERT}_B,\ \mathsf{sig}(\mathsf{sk}_B,(g^x,g^y))} & \\ & \xrightarrow{A,\ \mathsf{CERT}_A,\ \mathsf{sig}(\mathsf{sk}_A,(g^x,g^y))} & \end{array}$$

The result is a shared secret $K_{AB} = g^{xy}$ from which the parties derive a session-key.

(a) Briefly explain the purpose of the signatures in the protocol above. How does it defend against the attack discussed in class?

(b) Show that an active man-in-the-middle, Eve, can cause:

- A to think that she is communicating securely with B (as required),
- but B to think he is communicating securely with Eve.

In other words, B is fooled into thinking that the subsequent encrypted messages he is receiving (from A) are coming from Eve. Note that Eve cannot eavesdrop on the resulting encrypted channel.
Hint: Eve replaces the third message. You may assume that Eve also has a certificate, CERT_E, on her public signature verification key sk_E.

(c) Describe how Eve can use this attack to steal money from A. For example, suppose A gives expert advice in a private chat room run by B, and that she gets paid for that.

(d) Propose a way to fix the protocol to defend against this attack. Explain why your fix prevents the attack from Question 4(b).