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. You can expect to spend about 10 hours on this exercise, plus time for the required reading. The deadline for completing this coursework is **16:00, 10th March 2014**. 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 text books that are cited in the lecture slides.

Question 1

Here are some parameters for the ElGamal algorithm:

$$\begin{aligned} p &= 63689 && (modulus) \\ g &= 14569 && (generator) \\ k &= 11636 && (privat\,key) \end{aligned}$$

a) Check that these parameters fullfil the requirements for the ElGamal algorithm

b) Using these parameters, find the decryption of the ciphertext

$$(c1, c2) = (7265, 44824)$$

Show the calculations performed.

[*4 marks*]

To solve the question you may be able to find a suitable calculator or use the following Python functions, some from the gmpy library:

`gmpy.mpz(x)`	Create a gmpy integer with value x (this will allow you to perform fast exponentiation)
`gmpy.gcdext(x,y)`	Runs the extended euclidean algorithm on x and y. (i.e., find a and b such that $ax + by = gcd(x, y)$)
`pow(x,y,z)`	Computes x^y mod z.

Question 2

This question discusses notions of security.

(a). **Perfect security**: A system is perfectly secure if an attacker with infinite computing power can't learn anything about the message given the ciphertext. More precisely, a cipher (E, D) is perfectly secure if for any plaintext m and any ciphertext c, there exists a key k such that $c = E(k, m)$.

Outline how you would turn AES-CBC into a perfectly secure system.

(b). **Ciphertext indistinguishability**: A cipher (E, D) is said to satisfy plaintext indistinguishability if given two messages, a public key and a ciphertext (which is the encryption of one of the messages under the public key), an attacker can't decide which message was encrypted with a probability greater than 0.5. (Assuming a polynomially bounded adversary)

Do raw RSA and ElGamal satisfy this property?

(c). **Malleability**: A cipher (E, D) is said to be malleable if given the plaintext m_1 and the ciphertext c_1 under key k, it is possible to produce a ciphertext c_2 that decrypts to a message m_2 using k.

Show that ElGamal is malleable.

(d). **Plaintext awareness**: A cipher (E, D) is said to be plaintext aware if it is computationally difficult to construct a valid ciphertext c under key k without knowing the original message m.

While decrypting with RSA-OAEP, when are ciphertexts rejected? [*8 marks*]

Question 3

Notations $\mathsf{aenc}(k, m)$ (*resp.* $\mathsf{senc}(k, m)$) denotes the asymmetric (*resp.* symmetric) encryption of the message m under the key k. $\mathsf{sign}(k, m)$ denotes the signature with key k of the message m. $m_1 || m_2$ denotes the concatenation of message m_1 with message m_2.
An early version of SSL included the following authentication and key agreement protocol:

$$\begin{array}{ccccl} A & \rightarrow & B & : & Hello \\ B & \rightarrow & A & : & \mathsf{pbk}(B), Cert_B \\ A & \rightarrow & B & : & \mathsf{aenc}(\mathsf{pbk}(B), A || K) \\ B & \rightarrow & A & : & \mathsf{senc}(K, N) \\ A & \rightarrow & B & : & \mathsf{senc}(K, Cert_A || \mathsf{sign}(\mathsf{pvk}(A), N)) \end{array}$$

where K is a fresh session key generated by A, N is a fresh nonce generated by B, and $Cert_A$ and $Cert_B$ are certificates for A and B's public keys respectively.

(a). This protocol is flawed. Describe an attack on the protocol.

(b). Fix the protocol by changing it as little as possible. [*7 marks*]

Question 4

Design a protocol to

(a). generate a ”random” number over the phone, which cannot be forced by any of the participants. (The random number does not have to be secret)

(b). play rock-paper-scissors in a chat.

For each protocol discuss the properties needed and argue how your proposal achieved them.
For each protocol provide the requirements, the assumptions and the protocol steps. [*6 marks*]

Submission Instructions

You should submit your answers in person on hardcopy, either a printed document or a solution in clearly legible handwriting marked with your matriculation number at the top of each page.

Please submit the ITO by the deadline of **16:00, 10th March 2014**.

You're reminded that **late coursework** is not allowed without "good reason", see

`http://www.inf.ed.ac.uk/teaching/years/ug3/CourseGuide/coursework.html`

for more details about this, and the procedure to follow if you must submit late. In particular, if you have a good reason to submit late, please use the ITO support form to make a request.

Myrto Arapinis and Daniel Franzen
17th February 2014
2014/02/16 15:00:00.