Homework 3: Certificates and Public Key Crypto
These are practice problems that will not be graded.

February 26, 2015

Exercise 1. Key Exchange. This is a puzzle that allegedly inspired Diffie to invent a key exchange protocol.

1. Alice has an unopenable safe with a hook for a padlock. Alice wants to send Bob a diamond, but the post office will copy any key she sends. The post office will not open the safe, however, without a copy of the key. How can Alice do this?
2. Explain the analogy between the Diffie-Helman key exchange protocol and your solution to the puzzle above.
3. Explain why the messages exchanged in a Diffie-Helman key exchange protocol must be signed. If they were not, what sort of attacks could a man-in-the-middle adversary perform?

Exercise 2. Flame, and the hash-and-sign paradigm. In 2012, the Flame malware hijacked machines by coopting Microsoft's windows update software. Do some reading online to understand the incident.

Here is a gentle introduction:

`http://www.forbes.com/sites/richardstiennon/2012/06/14/`
`flames-md5-collision-is-the-most-worrisome-security-discovery-of-2012/`

Here is a detailed technical analysis:

`http://trailofbits.files.wordpress.com/2012/06/flame-md5.pdf`

You are welcome to read any article you like, as long as you cite your sources. The attack was based on finding a collision in the digital signature used to sign microsoft's code signing certificate.

1. Explain what a code-signing certificate is.
2. Why does forging the digital signature used to signed a code-signing certificate allow the attacker to take over the user's machine?
3. The digital signature used on the compromised certificate was "MD5-RSA" used in the hash-and-sign paradigm we discussed in class. Write down the signing algorithm and the verification algorithm.

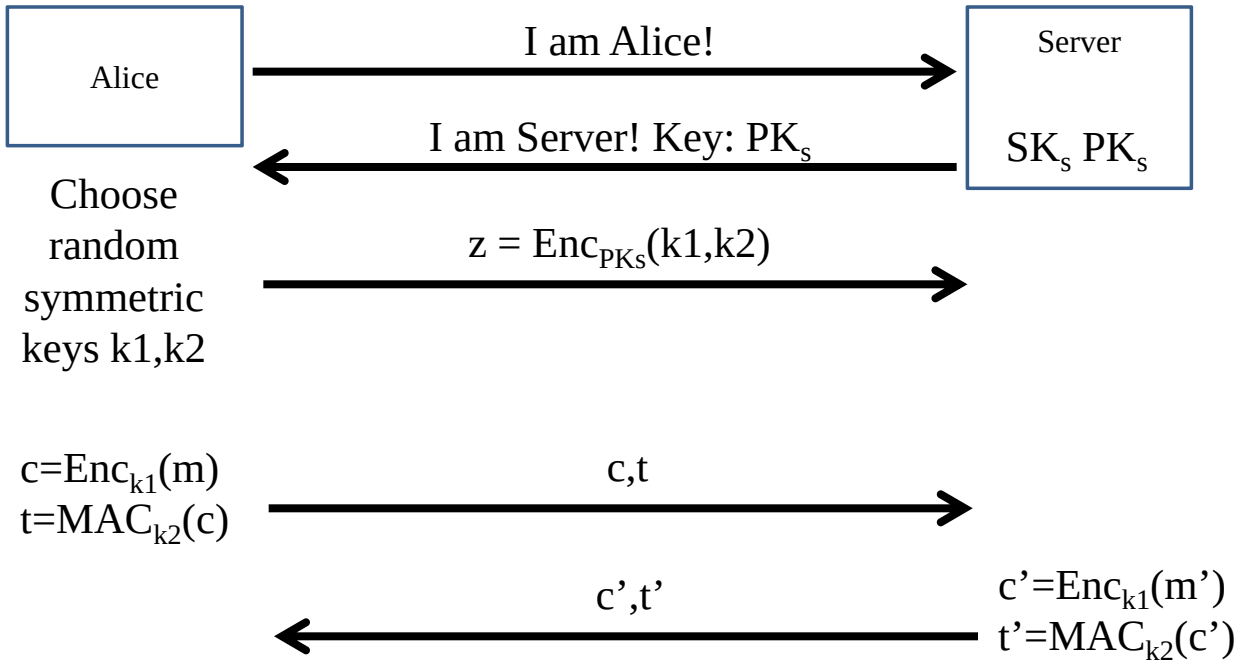
4. Explain the nature of the collision that the attackers found in MD5, and why that allowed them to create a bogus certificate.

5. In 2012, security researchers postulated that Flame was designed by a nation-state attacker. Explain why.

Exercise 3. (From 2014 midterm) This product is marketed as a new way to set up a secure channel.

Alice wants to send a message m to the server, and the server wants to respond with a message m'. The communication should be confidential, and no man-in-the-middle should be able to tamper with the communication.

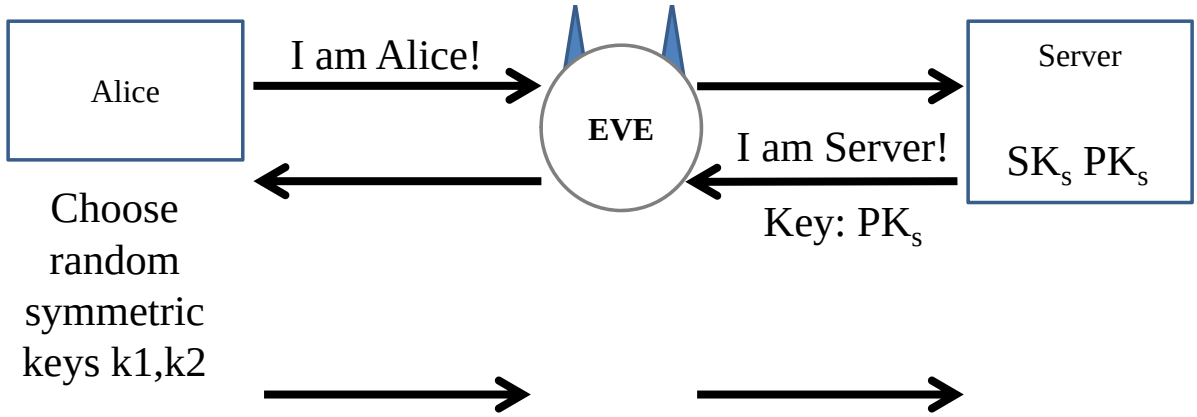
The server chooses a public-private key pair (SK_s, PK_s) and keeps SK_s secret.
Alice and the server then communicate as below:



1. **(2 points).** Write down the algorithm the server uses to recover m.

2. **(6 points).** Suppose Eve launches a man-in-the-middle attack; she sits on the communication path between Alice and the server, as shown below.

   Show how Eve can learn the messages m and m'.
   To do this, **draw the messages** Eve sends and receives from Alice and the Server, as well as **the computation** she performs in order to learn the messages. We started you off by drawing some, but NOT all, of the arrows involved in the communication.



3. **(3 points).** You use responsible disclosure to disclose this attack to Dr. Snakeoil, and he promises to fix the problem by requiring the addition of a new message, as follows:

   Now, right after the server receives the message $z = \mathsf{Enc}_{PKs}(k1, k2)$ from Alice, the server sends Alice a tag t which is computed as

$$t = MAC_{k_2}(\text{“Alice”}, \text{“Server”}, \mathsf{Enc}_{PKs}(k1, k2))$$

   Does this prevent the man-in-the-middle attack you came up with in Part (b)?
   Explain why or why not.