Security and Cryptography (CSS 322)

Assignment 2

Updates

- Update 4 (11 Feb 2008): added the email I sent to all students for your reference.
- Update 3 (10 Feb 2008): updated the certificate information to include the correct values of the messages and signatures that you should have sent to your partner. Use this information, not the emails!
- Update 2 (2 Feb 2008): added the certificate information, as well as updated the explanation of this information (and how you use it) here. Also, the Task 1 marks have been posted.
- Update 1 (27 Jan 2008): changed the example source code to explicitly set variables e, d, n, p and q as strings in the public/private key. Hence, my published key also changed.

Task 1

Complete the following steps:

1. Implement RSA in PHP. See the instructions for using PHP, as well as the template source code for detailed guidelines and conditions. (Note: after downloading the source code, change the file extension from .txt to .php).
2. Generate your own RSA keys (using your PHP code).
3. Submit your Public Key and source code via email to steve.siit@gmail.com by 8:00am Friday 1 February 2008. The email must containing the following (where you replace the example ID 4812345678 with your ID number):
   - Subject: `CSS322 Assignment 2 Task 1: 4812345678`
   - Body:

     ```
     ID: 4812345678
     Name: Steven Gordon
     Public Key: a:2:{i:0;s:3:"367";i:1;s:5:"15857";}
     ```

     Note that your public key is a serialized version of the public key data structure. See the template source code for instructions on how to generate this.
   - Attachment: your PHP code, with the file named as `a2-4812345678.php` (but using your ID number)

Task 2

By 5pm Monday 4 February 2008, I will publish all public keys on this website (here) in the form a (simplified) digital certificate. Each certificate will be a string of the form:

```
PublicKeyOfUser IDOfUser RSA_Encrypt(Hash_Simple(PublicKeyOfUser IDOfUser),PrivateKeyOfSt
```

where:

- `PublicKeyOfUser` is your Public Key in serialized form
- `IDOfUser` is your ID
- `PrivateKeyOfSteve` is my Private Key. My Public Key, in serialized form, is:

```
a:2:{i:0;s:3:"367";i:1;s:5:"15857";}
```

- `RSA_Encrypt()` and `Hash_Simple()` are two PHP functions in your assignment source code.
- Note that the items are separated by a single space.

Complete the following steps:

1. Download the certificate of another user (known as your *partner*).
2. Validate the certificate of your partner using `RSA_ValidateCertificate()` (you have to write the `RSA_Validate()` function yourself - you will also have to write `RSA_Sign()` for the next part).
3. Using RSA send a signed and encrypted message to your partner via email and CC the email to: me at steve.siit@gmail.com; and to your *malicious user* by 8:00am Friday 8 February 2008. The email must containing the following (of course replacing the data with the appropriate values):
   - Subject: `CSS322 Assignment 2 Task 2: 4812345678`
   - Body:

     ```
     FromID: 4812345678
     FromName: Steven Gordon
     ToID: 4800000000
     Message: 4315345 63
     ```

     The signed and encrypted message is of the format: `Ciphertext RSA_Encrypt(Hash_Simple(Ciphertext),Key)`.

The certificates file contains the following information:

- User X's ID, name and email address
- User X's certificate, that is, user X's public key signed by the Certificate Authority. Note that I have formatted the public keys to be a common format, and for several people (those that submitted incorrect or bad public keys in Task 1) I have created new public keys (those people received their public/private key by email from me).
- The ID of the partner for user X. User X can obtain their partners name, email and certificate from the list.
- An encrypted form of the message that user X will send to their partner. This is encrypted by me (the CA) so that only user X can get the original message. This message is not signed by me.
- The ID of the malicious user for user X. User X can obtain the email address of the malicious user from the list.

Task 3

Complete the following steps:

1. Validate and decrypt the message from your partner.
2. Write the function `RSA_Attack()` that a malicious user can apply to try to discover a plaintext message (from a captured ciphertext, and any other public information). Try to develop a generic function which will work efficiently for many different input values (e.g. larger than the values used in this assignment).
3. Apply `RSA_Attack()` to determine the plaintext for the message you intercepted as a malicious user (that is, the email that you were CCed from the other user in Task 2). Note that, your attack can only make use of the information that normally would be publicly available to a malicious user (that is, you cannot simply ask your friend what the plaintext is!).
4. Answer the following questions (your answers should be clear and detailed, so that another 3rd/4th year ICT student that hasn't studied CSS322 could understand them - you may use diagrams and examples in your answers):

   1. Explain how you validated the certificate in Task 2 (and why you know it is or is not valid). Include a discussion of the assumptions that were made for this to work.
   2. Discuss the Hash function used, including its strength and/or weaknesses. Your discussion should evaluate the Hash function against the desired properties (requirements) of a hash function.
   3. Explain an example of how an attacker could take advantage of the weakness of the Hash function, including what malicious activity they could perform and how.

5. Submit a hardcopy of a written (or printed) report to me by 9:00am Friday 15 February 2008 (start of the lecture) that contains:
   - Cover page (with name, ID, course, etc.).
   - Answers to the questions in the above point.
   - Printout of all of your PHP code (that is, print out of `a2-4812345678.php`).
6. Email a copy of your PHP code to me at steve.siit@gmail.com by 8:00am Friday 15 February 2008. The email must containing the following (where you replace the example ID 4812345678 with your ID number):
   - Subject: `CSS322 Assignment 2 Task 3: 4812345678`
   - Body:

     ```
     ID: 4812345678
     Name: Steven Gordon
     ```

   - Attachment: your PHP code, with the file named as `a2-4812345678.php` (but using your ID number)

Marking Scheme

- `RSA_Encrypt()` and `RSA_Decrypt()`: 10 marks
- `RSA_GenerateKeys()`: 10 marks
- `RSA_Validate()` and `RSA_Sign()`: 10 marks
- `RSA_Attack()`: 10 marks
- Written questions: 15 marks
- Following instructions, good code, etc.: 5 marks
- TOTAL MARKS: 60

Return to: Course List | Steven Gordon's Home | SIIT