Lab 13 – Online Gaming Technologies

Josh Tyrrell Browne

C00224660

Question information:

Alice and Bob wish to communicate with each other over the Internet. Each uses RSA, the common asymmetric cryptography protocol. Thus, each has his/her own private key and knows the public key of the other. Let us denote private key of Alice as Pr(A), private key of Bob as Pr(B), public key of Alice as Pu(A), and public key of Bob as Pu(B).

Question 1:

Alice wants to send a message to Bob so that no one else can read it. Let us denote the message as M_1. How would Alice send the message?

Answer 1:

Alice must know Bob's public key to encrypt the message, so that Bob can decrypt the message using his secret key. The following steps are how Alice would send a message to Bob, whilst ensuring nobody else could intercept and decrypt:

1. Bob sends Alice his public key (Pu(B)) via a reliable, but not necessarily secret, route. (Bob's secret key Pr(B) is never distributed)
2. Alice firstly transforms her message "M_1" into a padded version of the message by using an agreed upon reversable protocol (i.e padding scheme)
3. Alice then transform's padded version of "M_1" to ciphertext using "Pu(B)". This operation can be shown in the following formula: M_1 ^ (Pu(B)) = ciphertext
4. Alice then sends this ciphertext to Bob. (Bob's private key, which only he has, is what is needed to decipher the ciphertext.)

Question 2:

Let us denote the message Alice sent as M_3. How would Bob decipher the message?

Answer 2:

Bob can decipher the message using Pr(B). The following steps are how this would be done:

1. Bob uses the following formula to decrypt the message:
   M_3(aka ciphertext) ^ Pr(B) = M_1(padded)
2. Bob then reverses the padded scheme on the result and he then has the original "M_1" message sent by Alice.

Question 3:
In this situation, Alice does not care if anyone can read her message. But she does care that no one in the middle can change the message (in an undetectable manner). Let us denote the message as M_2.
How would Alice send the message?
What would Bob do to verify that the message indeed came from Alice?

Answer 3:
This question is about how we can verify that a message definitely came from a particular person. RSA has a way of doing this verification and it is called “signing a message”. This is essentially done by the sender attaching a hash value of the message raised it to the power of their own private key. Then, once the receiver receives the signed message, they can use the same hash algorithm in conjunction with the sender's public key to verify that the message was signed using the senders private key and can then be sure that the message was not changed and is the original and authentic message from the sender.

How Alice would send the message:

1. Alice produces a hash value of the message.
2. She then raises it to the power of Pr(A).
3. She then attaches this as a “signature” to the message.

How Bob verifies that the message is authentic and un-tampered:

1. Bob uses the same hash algorithm in conjunction with Pu(A).
2. He then raises the signature to the power of Pu(A).
3. He compares the resulting hash value with the “M_2” hash value. If the two agree, he knows that the author of the message was in possession of Alice’s private key.

This all works because of exponentiation rules:
H = hash(m)
(H^Pr(A)) ^ Pu(A) = H^ (Pr(A))(Pu(A)) = H^ (Pu(A))(Pr(A)) = (H^Pu(A)) ^ Pr(A) = H (mod n)