Information Security Technologies COMP607 Tutorial

Session 4 Asymmetric Key Cryptography -- RSA

1. Test Euler’s theorem with some simple examples.
   1. Choose a number n < 100.
   2. Obtain Φ(n) by counting the number of integers that is relatively prime to n.
   3. Choose a number M< 100 and show that MΦ(n) mod n = 1
2. Work in pairs, each person:

Choose two prime number *p,q* < 100, compute *n = pq*

Compute Φ(*n*) = (*p-1*)(*q-1*)*;* discard *p, q*

By trial and error choose *e,d < Φ*(*n*) such that *ed ≡ 1* mod Φ(*n*) , i.e. *ed* = 1+*k*Φ(*n*)

Give your partner your public key <*e,n*>, keep your private key <*d,n*> secret

1. Encryption messages to each other:

Choose a message *M* < *n*, that is relatively prime to n and encrypt it using *C = Md* mod

*n* and give it to your partner.

Decrypt each other’s cipher text using *Cd* mod *n*. Can you get the correct message?

Repeat with a message *M* that is not relatively prime to *n.* Can you correctly decrypt the message?

1. Signatures:

Choose a message *M* < *n* to sign, (note that *M* must be relatively prime to *n*). Normally the message digest is obtained using a hash function. To keep things simple and avoid large numbers, just by sign the message by computing *sig* = *Md* mod *n*. Give {*M, sig*} to your partner.

Verify your partner’s signature, *sig* using his/her public key *e*, by computing *sige* mod *n*

and comparing to *M.* Is the signature it verified?

1. Breaking RSA using some simple methods. Given your partner’s public key <*e,n*> try to compute his/her private key *d,* e.g. by guessing the value of Φ(*n*), factorizing *n*, etc.
2. One of the most attractive applications of public-key algorithms is the establishment of a secure session key for a private-key algorithm such as AES over an insecure channel. Assume Bob has a pair of public/private keys for the RSA cryptosystem. Develop a simple protocol using RSA which allows the two parties Alice and Bob to agree on a shared secret key. Who determines the key in this protocol, Alice, Bob, or both?