Information Security Technologies COMP607
Tutorial

Session 4 Asymmetric Key Cryptography -- RSA

1. Test Euler's theorem with some simple examples.
   a. Choose a number n < 100.
   b. Obtain Φ(n) by counting the number of integers that is relatively prime to n.
   c. Choose a number M< 100 and show that
      $M^{\Phi(n)} \bmod n = 1$

2. Work in pairs, each person:
   Choose two prime number $p,q < 100$, compute $n = pq$
   Compute $\Phi(n) = (p-1)(q-1)$; discard p, q
   By trial and error choose $e,d < \Phi(n)$ such that $ed \equiv 1 \bmod \Phi(n)$, i.e. $ed = 1+k\Phi(n)$
   Give your partner your public key <*e*,*n*>, keep your private key <*d*,*n*> secret

   (a). Encryption messages to each other:
   Choose a message $M < n$, that is relatively prime to n and encrypt it using $C = M^d \bmod n$ and give it to your partner.
   Decrypt each other's cipher text using $C^d \bmod n$. Can you get the correct message?

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

   (b). 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 $sig = M^d \bmod n$. Give {*M*, *sig*} to your partner.

   Verify your partner's signature, *sig* using his/her public key *e*, by computing $sig^e \bmod n$ and comparing to *M*. Is the signature it verified?

   (c). 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.

3. 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?