Operating Systems - Week 8 Tutorial

(with acknowledgement to Roger England.)

Q1. Ali wants to buy cinema tickets from www.moviellink.com. However, he does not want to give out his credit card number to Moviellink. Ali and the Moviellink have the same bank. For the bank to transfer money from Ali's account to Moviellink's account, it needs to know Ali's account number, Moviellink's account number, and the amount. Ali is able to digitally sign the request for bank to honour it, but Moviellink does not want to give its account number to Ali.

A system is designed whereby Ali sends a message to Moviellink containing his account number and the transfer amount. Moviellink forwards this message to the bank after appending its own account number to it:

Ali → MovieLink: Ali's account number, £amount
MovieLink → Bank: Ali's account number, £amount, MovieLink’s account number.

The communication channels are not safe. For example, the message sent to Moviellink by Ali can be intercepted and forwarded to the bank with a bogus account number. Or the message sent by Moviellink to the bank may be captured and modified.

Using public key encryption, sort out what individual fields, groups of fields and entire messages need to be signed and/or encrypted and state whose public and/or private key is used so that:

• The bank should be able to see all three fields and perform the transfer.
• Moviellink should not be able to see Ali's account number.
• Moviellink should be able to verify the amount.
• Moviellink should not be able to change it.

Assume that the public keys of all parties are known to all other parties, including any message interceptors. Each party also knows their own private key and no other. There are no other shared secrets between parties.

NB A public key is one which everyone knows (based for example on the product of two large prime numbers). A private key is known only to the decrypter (for example the prime numbers forming the product) and is the INVERSE of the public key in the sense that they all have the property:

public_key(private_key(message)) = private_key(public_key(message))

= message,

so that private keys can be used for encryption or decryption (and similarly for public keys). The latter is the basis for digital signatures.

Q2. We can construct a bare bones RSA public key cryptosystem. Assume we use an alphabet coding of $A=1, B=2, C=3, \ldots Z=26$. We choose two primes: $p=3$ and $q=11$, then $n = p \times q = 33$. (See end of Qn for method of computing $e, d$.)
p = 3 is the first prime number (destroy this after computing $e$ and $d$)
q = 11 is the second prime number (destroy this after computing e and d)  
pq = 33 is the modulus (give this to others)  
e = 3 is the public exponent (give this to others).  
d = 7 is the private exponent (keep this secret!)  
Your public key is (pq,e). Your private key is d.  
T, C is text and t, c its numeric equivalent so  
The encryption function is: encrypt(T) = (t^e) mod pq = (t^3) mod 33  
The decryption function is: decrypt(C) = (c^d) mod pq = (c^7) mod 33  
The following table should show you how to do the encryption/decryption:

<table>
<thead>
<tr>
<th>encrypt</th>
<th>T</th>
<th>plain (t)</th>
<th>T^-3</th>
<th>T^-3 mod 33</th>
<th>cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>18</td>
<td>5832</td>
<td>24</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>15</td>
<td>3375</td>
<td>9</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>7</td>
<td>343</td>
<td>13</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>5</td>
<td>125</td>
<td>26</td>
<td>Z</td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>18</td>
<td>5832</td>
<td>24</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>decrypt</th>
<th>C</th>
<th>cypher</th>
<th>C^-7</th>
<th>C^-7 mod 33</th>
<th>plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>24</td>
<td>4586471424</td>
<td>18</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>I</td>
<td>9</td>
<td>4782969</td>
<td>15</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>13</td>
<td>62748517</td>
<td>7</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Z</td>
<td>26</td>
<td>8031810176</td>
<td>5</td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>24</td>
<td>4586471424</td>
<td>18</td>
<td>R</td>
<td></td>
</tr>
</tbody>
</table>

Write a (short!) message to your neighbour, encode it, and decrypt theirs  
(a calculator is available on the sun machines).  
Note for the interested: d and e are chosen as follows. Form some primes  
which are less than z , where z = (p - 1) × (q - 1).  
Here d=7 is a suitable prime. Obtain e from e × d = 1 mod (z), so  
7e = 1 mod (2) and therefore e = 3.