Problem Set 6  (Solutions are due Fri. 3-14-08)

1) RSA Encryption and Decryption. To practice encryption and decryption of text with numbers that can be handled easily in Matlab, consider the following conversion from text to integers and vice versa. Each text character is encoded using the standard 7-bit ASCII code, resulting in a decimal number in the range 0 . . . 127. Let \((x_0, x_1, x_2)\) represent a sequence of three characters \((x_0\ \text{followed by}\ x_1, \ \text{followed by}\ x_2)\). To convert them to a plaintext message integer \(m\), \(0 \leq m < 2^{25}\), the following formula is used

\[
m = (x_0 2^{14} + x_1 2^7 + x_2) 2^4.
\]

The purpose of the overall multiplication by \(2^4\) is to add some redundancy, so that a “legal” plaintext can be distinguished from an arbitrary string.

Example: The text \texttt{ToyRSA} is converted to two plaintext integers \(m\) as follows:

<table>
<thead>
<tr>
<th>ASCII char</th>
<th>T</th>
<th>o</th>
<th>y</th>
<th>R</th>
<th>S</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>decimal value</td>
<td>84</td>
<td>111</td>
<td>121</td>
<td>82</td>
<td>83</td>
<td>65</td>
</tr>
<tr>
<td>corresponding (m)</td>
<td>22249360</td>
<td>21666832</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(a) Using the text to plaintext integer conversion outlined above, encrypt the plaintext \texttt{Stanislav} with the public key \(n = 46885453\) and \(e = 23567473\).

(b) Decipher the following sequence of three ciphertext numbers and convert them back to text using the conversion explained above.

\[
c_a = 8234303 \quad c_b = 575488 \quad c_c = 6491872
\]

The public key that was used for encryption is \(n = 51926723\) and \(e = 36830249\).

2) The following randomized algorithm can be used to compute square roots modulo \(p\) where \(p\) is an odd prime number.

Input: Odd prime \(p\), integer \(a \in QR_p\).

Output: \(x = \sqrt{a}\).

1. Write \(p - 1 = 2^s \ m, \ m\ \text{odd}.\)
2. Select random \(b \in \mathbb{Z}_p^*\) until one is found with \(L(b, p) = -1\) (i.e., \(b \in QNR_p\)).
3. Compute \(a^{-1} \pmod{p}\).
4. Set \(d \leftarrow b^m \pmod{p}\) and \(x \leftarrow a^{(m+1)/2} \pmod{p}\).
5. For \(i = 1\) to \(s - 1\) do:
   5.1 \(y = (x^2 a^{-1})^{2^{s-i-1}} \pmod{p}\).
5.2 If \( y = -1 \pmod{p} \) set \( x \leftarrow x d \pmod{p} \).
5.3 Set \( d \leftarrow d^2 \pmod{p} \).
6. Return \((x, -x)\).

Use this algorithm to compute the following square roots:

(a) \( a = 37041386, p = 91301009, x = \sqrt[2]{a} \pmod{p} \).
(b) \( a = 80570093, p = 90158491, x = \sqrt[2]{a} \pmod{p} \).
(c) \( a = 5115781, p = 88368733, x = \sqrt[2]{a} \pmod{p} \).
(d) \( a = 227487, p = 23068673, x = \sqrt[2]{a} \pmod{p} \).
(e) What are the different features of the algorithm that each of these examples is testing?

3) Rabin Encryption and Decryption. Use the basic Rabin cryptosystem (given in the Appendix) which computes \( c = m^2 \pmod{n} \), with \( n = pq \), \( p, q \) odd primes.

(a) Using the text to plaintext integer conversion outlined in problem 1, encrypt the plaintext \textit{bloodshed} with the public key \( n = 36909151 \).

(b) Decipher the following sequence of three ciphertext numbers and convert them back to text using the conversion explained in problem 1.

\[
c_a = 52408378 \quad c_b = 64655092 \quad c_c = 38704627
\]

The public key that was used for encryption is \( n = 72809999 \).

Appendix: Rabin Cryptosystem

The basic Rabin public key cryptosystem is set up as follows:

1. Let \( n = pq \) where \( p \) and \( q \) are two distinct large primes chosen such that factoring \( n \) is computationally infeasible.
2. The public key is \( n \) and the private key is \((p, q)\).

If \( B \) encrypts a message \( m \) for \( A \), the basic Rabin cryptosystem is used as follows:

1. \textit{Encryption}. \( B \) does the following:
   1.a Obtain \( A \)'s authentic public key.
   1.b Represent the message as an integer \( m, 0 \leq m < n \).
   1.c Compute \( c = m^2 \pmod{n} \).
   1.d Send ciphertext \( c \) to \( A \).

2. \textit{Decryption}.
   2.a Compute the 4 square roots \( m_1, m_2, m_3, m_4 \) of \( c \) modulo \( n \).
   2.b Plaintext \( m \) is one of the 4 square roots (typically some redundancy is added to \( m \) so that it can be recognized as the “right” square root).