Introduction to Cryptography

Midterm 1

November 8, 2006

NAME: .....

problem	1	2	3	4	5	6	7
points to earn	10	20	10	10	30	10	10
points earned							

1. Solve the following cryptogram:

   NOVSG XJ NOQ QMPNO MD M WVCVSI XPIMSVDU NOMN VD LQVSI MNNMKGQT LZ

   LVWWVXSD XJ LMKNQPVM BOXDQ SRULQPD TXRLWQ QCQPZ JXPNZ ZQMPD.

   IXPQ CVTMW

   Explain your first steps.

2. Explain how RSA works. How do you pick the parameters p, q, N, d, and e? What is the private and public key? How are messages encrypted and decrypted? Why does it work?

3. In the proof that RSA works, you have used the Theorem of Euler-Fermat, which is only valid if $\gcd(m, N) = 1$. Show that the RSA-protocol even works if $\gcd(m, N)$ is nontrivial.

4. We have shown that the complexity of (naive) addition, multiplication and division in terms of bit operations is as follows:

operation	complexity
$a + b$	$O(\max\{\log a, \log b\})$
ab	$O(\log a \cdot \log b)$
$a = bq + r$	$O(\log b \cdot \log q)$

Estimate the number of bit operations to compute the left side and the right side of the equation

$$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}.$$

5. The Paillier cryptosystem works as follows: Alice picks distinct primes p and q, computes $n = pq$, and determines an integer a with $an \equiv 1 \bmod \phi(n)$. The public key is n, the private key is a.

   To encrypt a message $m < n$, Bob picks a random integer $r < n$ coprime to n, computes $c \equiv (1+n)^m r^n \bmod n^2$, and sends c to Alice.

   For decrypting c, Alice computes the smallest positive $R < n$ with $R \equiv c^a \bmod n$, $z \equiv cR^{-n} \bmod n^2$, and finally $M = \frac{z-1}{n}$.

   (a) Show that $c \equiv r^n \bmod n$.

   (b) Show that $R = r$.

   (c) Show that $(1+n)^m \equiv 1 + mn \bmod n^2$.

   (d) Show that $M = m$ (in particular, anyone knowing a can decrypt the cipher texts c).

   (e) Show that Eve can break the Paillier system if she can factor n.

   (f) Show that the Paillier cryptosystem is *additively homomorphic*, i.e. that if c_1, c_2 are encryptions of m_1 and m_2, then $c_3 \equiv c_1 c_2 \bmod n^2$ is an encryption of the message $m_3 \equiv m_1 + m_2 \bmod n$.

6. Bob computes $2^{n-1} \bmod n$. What conclusions can Bob draw if he finds that $2^{n-1} \not\equiv 1 \bmod n$? What if $2^{n-1} \equiv 1 \bmod n$?

7. Describe Pollard's rho method for finding prime factors p of composite integers. What is the connection with the birthday paradox?