PMAT 669 Public Key Cryptography

Assignment 2

Set Oct 12, 2005 **Due Oct 26, 2005**

[2] 1. Use the extended Euclidean algorithm to compute $355^{-1} \pmod{1234}$.

[2] 2. Solve the following system of congruences

$$\begin{aligned} x &\equiv 12 \pmod{25} \\ x &\equiv 9 \pmod{26} \\ x &\equiv 23 \pmod{27} \end{aligned}$$

[2] 3. Compute the Jacobi symbol

$$\left(\frac{1234567}{11111111}\right)$$

[3] 4. Show that if k is the number of distinct prime factors of $n > 1\,(n \text{ odd})$, then $x^2 = 1 \bmod n$ has exactly 2^k distinct modulo n solutions. Hint: use the Chinese Remainder Theorem.

[4] 5. Show how to find $n-th$ roots modulo p quickly, assuming the existence of a fast routine which finds $n-th$ roots when $n \mid p-1$.

[4] 6. Give a polynomial time algorithm that on input $n > 1$ finds $b, c > 1$ such that $n = b^c$ if such b, c exist.

[3] 7. This exercise exhibits what is called a *protocol failure*. It provides an example where ciphertext can be decrypted by an opponent, without determining the key, if a cryptosystem is used in a careless way. (Since the opponent does not determine the key, it is not accurate to call it cryptanalysis.) The moral is that it is not sufficient to use a "secure" cryptosystem in order to guarantee "secure" communication.

Suppose Bob has an **RSA Cryptosystem** with a large modulus n for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 (i.e. , $A \leftrightarrow 0, B \leftrightarrow 1$, etc.), and then encrypting each residue modulo 26 as a separate plaintext character.

(a) Describe how Oscar can easily cryptanalyze a message which is encrypted in this way.

(b) Illustrate this attack by decrypting the following ciphertext (which was encrypted using an **RSA Cryptosystem** with $n = 18721$ and $b = 25$) without factoring the modulus:

$$365, 0, 4845, 14930, 2608, 2608, 0.$$