密碼學與應用作業(三)

2005/12/22

1. (Trappe 2nd Ed. 6.8.3 modified)
   The ciphertext 229 was obtained using RSA with n = 437 and e = 3. Suppose you know that the plaintext is either 68 or 69. Determine which it is without factoring n. (Note: you probably do not need to do any modulo exponentiation computations.)

   Sol:
   Because RSA encryption is a permutation (it means that RSA encryption is 1-1 (if x $\neq$ y then f(x) $\neq$ f(y)) and onto (f: X → Y is onto iff for all y in Y, there exists x in X, s.t. f(x)=y) function mapping from the message space to the ciphertext space), we can use this property to solve it.
   It is clear that $69^3 \pmod{437}$ is an even number, therefore, $68^3 \pmod{437}$ must be 229, i.e., the plaintext is 68.

2. (Trappe 2nd Ed. 6.8.11)
   Suppose that there are two users on a network. Let their RSA moduli be n_1 and n_2, with n_1 not equal to n_2. If you are told that n_1 and n_2 are not relatively prime, how would you break their systems?

   Sol:
   n = p · q; p,q $\in$ Prime number

   $\because$ n_1, and n_2 are not relatively prime
   $\therefore$ we can break n_1 ,and n_2
   gcd(n_1 , n_2) = p
   q_1 = n / p , and q_2 = n / p
   we can factor n_1 = p · q_1 and
   n_2 = p · q_2

3. (Trappe 2nd Ed. 6.8.13)

Suppose you discover that

$$880525^2 \equiv 2, 2057202^2 \equiv 3, 648581^2 \equiv 6, \text{ and } 668676^2 \equiv 77 \pmod{2288233}$$

How would you use this information to factor 2288233? Explain what the steps you would do, but do not perform the numerical calculations.

Sol :
$880525^2 \cdot 2057205^2 \equiv 6 \equiv 648581^2 \pmod{2288233}$
$(880525 \cdot 2056205)^2 \equiv 648581^2 \pmod{2288233}$
but $880525 \cdot 2056205 \equiv 1517000 \not\equiv \pm 648581 \pmod{2288233}$
Therefore, either
gcd((880525 × 2056205 $\pmod{2288233}$) - 648581 , 2288233) or
gcd((880525 × 2056205 $\pmod{2288233}$) + 648581 , 2288233)
is the nontrivial vactor p, the other factor is 2288233/p.

4. (Trappe 2nd Ed. 6.8.15)
Suppose n is a large odd number. You calculate $2^{(n-1)/2}$ ≡k (mod n), where k is some integer with k≢ ±1 (mod n).

   (a) Suppose k^2 ≢1 (mod n). Explain why this implies that n is not prime.

   (b) Suppose k^2 ≡1 (mod n). Explain how you can use this information to factor n.

   Sol:

   (a) Since $2^{(n-1)} \equiv k^2 \not\equiv 1 \pmod{n}$
   From Fermat's Little theorem, we know that n is not a prime number.

   (b) $2^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$ and $2^{(n-1)} \equiv 1 \pmod{n}$
   From the "basic factoring principle", $k^2 \equiv 1^2 \pmod{n} andk \not\equiv \pm 1 \pmod{n}$
   we can find a nontrivial factor of n as gcd(k-1, n) or gcd(k+1, n)

5. (Trappe 2nd Ed. 6.8.20)
Suppose $n = p \cdot q \cdot r$ is the product of three distinct primes. How would an RSA-type scheme work in this case? In particular, what relation would e and d satisfy?

   Note: There does not seem to be any advantage in using three primes instead of two. The running times of some factorization methods depend on the size of the smallest prime factor. Therefore, if three primes are used, the size of n must be increased in order to achieve the same level of security as obtained with two primes.

In the case n = p q, we know that using CRT would cut the computation time of decryption into 1/4. If the smallest prime factor of the three factor scheme has the same length of the two factor scheme, show that CRT can only cut the computation time of decryption into 3/8, which is worse than the two factor scheme.

$\phi(n) = (p-1)\cdot(q-1)\cdot(r-1)$
$gcd(e, \phi(n)) = 1$ implies that there exists d such that
$e \cdot d \equiv 1 \pmod{\phi(n)}$
i.e. $d \equiv e^{-1} \pmod{\phi(n)}$

6. (Trappe 2nd Ed. 6.8.22)

   (a) Show that if gcd(e, 24) = 1, then $e^2 \equiv 1 \pmod{24}$.

   (b) Show that if n = 35 is used as an RSA modulus, then the encryption exponent e always equals the decryption exponent d.

   (a) $24 = 2^3 \cdot 3$, $\phi(24) = 2^3 \cdot 3 \cdot (1-\frac{1}{2}) \cdot (1-\frac{1}{3}) = 8$
   $Z^*_{24} = \{1, 5, 7, 11, 13, 17, 19, 23\}$
   It is easy to verify that for each element in Z^*_{24}, $e^2 \equiv 1 \pmod{24}$

   (b) step 1: n = 35 = 7·5
   step 2: Φ(35) = (7-1)·(5-1) = 24
   step 3: select a random integer e such that gcd(e , Φ(35)) =1
   step 4: calculate the unique integer d such that e·d = 1 (mod Φ(35))
   part (a) shows that d must equal to e.