MAS433 Cryptography: Tutorial 6
Public Key Encryption
28.10.2010

Instructions.

1. Submission of tutorial solution is compulsory.
2. Submission deadline: 27 October 2011, 6PM
3. Please submit your solution by sending email to wuhj@ntu.edu.sg (If your solution is handwritten, you can scan and convert it into digital format, such as .pdf document.)
4. Tutorial solution will not be provided after the tutorial class.

Question 1. Modified Diffie-Hellman Key Exchange Protocol
After having studied the Diffie-Hellman protocol, a cryptography amateur decides to implement it. In order to simplify the implementation, he decides to use the additive group $(Z_p, +)$ instead of the multiplicative one $(Z_p^*, \cdot)$. What do you think about the secuirty of this new protocol?

Question 2. Toy RSA
In a toy RSA encryption scheme, $n = 161$, $e = 5$. Find the value of the private key d. Decrypt the ciphertext $c = 3$.

Question 3. RSA: Padding

3.1 How to perform message padding in CBC mode, SHA-1, CMAC and RSA encryption?

3.2 Suppose that OAEP is used in RSA encryption. Is it secure to use small modulus n? Is it secure to use small public key exponent e? Is it secure to use small private key d? Is it secure to encrypt a small plaintext m? Explain why.

Question 4. RSA: $\lambda(n)$
In RSA, d can be computed as $e \cdot d \equiv 1 (\mathrm{mod} \lambda(n))$, where

$$\lambda(n) = \frac{(p-1)(q-1)}{gcd(p-1, q-1)}.$$

4.1 Prove that encryption and decryption are inverse operations. (Hint: How do we prove that the RSA encryption and decryption are inverse operations?)

4.2 Let $n = 161$, $e = 5$. Find the value of the private key d. Decrypt the ciphertext $c = 3$.

Question 5. RSA: Common Modulus
Two users Alice and Bob use RSA public keys with the same modulus n but with different public exponents e_A and e_B.

5.1 Prove that Alice can decrypt messages sent to Bob.

5.2 Suppose that message padding is not used in RSA encryption. Suppose that $\gcd(e_A, e_B) = 1$. A plaintext m was sent to Alice and Bob, encrypted using the public keys of Alice and Bob, respectively. Show that an attacker can find the plaintext m. (Hint: how to find a and b satisfying $a \times e_A + b \times e_B = 1$)

Question 6. (Bonus Question) RSA: small difference between p and q
The p and q in RSA should be randomly generated, and they are the same size. The difference between p and q should not be small.

6.1 Suppose that p and q are 1024-bit prime numbers, but the difference between p and q is small, say, $u = |p - q| < 2^{32}$. How to factorize the product of p and q?

6.2 Suppose that $u = |p - q| < 20$, and $p \times q = 2189284635403183$. Find the values of p and q.

Question 7. (Bonus Question) Dixon's Random Squares Algorithm
Factorize 256961 using Dixon's Random Squares Algorithm. The factor base {-1,2,3,5,7,11,13,17,19,23,29,31} may be used.

Question 8. Toy ElGamal Encryption
In a toy ElGamal encryption scheme, $p = 227$, $g = 2$, and $x = 15$. Decrypt the ciphertext (10, 159).