HW #4: Asymmetric Cryptography

CS 6903: Modern Cryptography
Spring 2008

[100pts] DUE 05/15/2009 (11am)

Problem 1 [15pts]

Argue why the following are true or false:

1. For x, y, a belonging to \(\mathbb{Z}_N^*\), does \(x = 2y \mod N\) \(\Rightarrow\ a^x = a^{2y} \mod N\)
2. For x, y, a belonging to \(\mathbb{Z}_p^*\), does \(2x = y \mod (p-1)\) \(\Rightarrow\ a^{2x} = a^y \mod p\)
3. It is possible to compute inverses modulo N, where N is a product of two large prime numbers (or say RSA modulus)? Assume N to be 1024-bit long.

Problem 2 [15pts]

1. Show why DDH is easy in \(\mathbb{Z}_p^*\)
3. Give two examples of groups where DDH is hard. Is CDH easy in such groups? Is DL easy in such groups? Why/why not?

Problem 3 [15pts]

2. What is the order of the group \(\mathbb{Z}_N^*\)? Work it out.
3. Can gcd(e, \(\Phi(N)\)) = 3? Why/why not? e is RSA exponent and N is RSA modulus.

Problem 4 [15pts]

3. Is it secure to use the same random value r, while encrypting two different messages m1, m2 for the same person? Argue why/why not.

Problem 5 [15pts]
1. Describe all steps involving certification of a person’s public key. Also, explain all steps in the verification of the certificate. (This also involves checking if a certificate is revoked or not, e.g., by periodically downloading a list of revoked certificates from a trusted authority).

2. Go to https://my.poly.edu, grab the digital Polytechnic certificate and answer these questions:
   a. Who has signed the certificate or who is the CA? Is the CA trusted?
   b. Has the certificate expired? Is the certificate revoked?
   c. What digital signature scheme is used to sign the certificate?
   d. What cryptosystem is used to generate the public (private) keys? What is the public key that’s being certified (just copy-paste it)?
   e. A general question: can the CA use a DL-based signature scheme to sign an RSA public key? Why/why not?

**Problem 6 [10pts]**

1. Give an example scenario to illustrate why CMA security notion for signature schemes is a practical notion.

2. What is the difference between the CMA security notion of a MAC and the CMA security notion of a digital signature? What is the reason for this difference?

**Problem 7 [15pts]**

1. Write down the “story” regarding OAEP (and RSA-OAEP) that I told you in the class. 😊

2. Refer to the Section 6 (“Instantiation”) of the paper http://www-cse.ucsd.edu/~mihir/papers/ro.pdf, and show how the functions G and H needed in the OAEP construction can be instantiated using, e.g., MD5 hash function.