HW #3: Message Authentication; Number Theory, Public-Key Cryptography

CS 6903: Modern Cryptography
Spring 2010

[150pts] DUE 05/14/2010 (11am)

Problem 1 [10pts]

Show that \( \text{NMAC}_{k_1,k_2}(x) = H(k' \xor \text{opad}, H(k' \xor \text{ipad})) \), where \( k_1 = h(k' \xor \text{opad}) \) and \( k_2 = h(k' \xor \text{ipad}) \). \( h() \) is the compression function that takes inputs of b-bit block of message and a L-bit chaining vector. \( k' \) is the key \( k \) padded with appropriate number of 0’s that makes it b-bit long. \( \text{ipad} \) and \( \text{opad} \) are paddings of b-bit block.

Mention one advantage and one disadvantage each of using HMAC and NMAC, in practice.

Problem 2 [20pts]

Consider the hash function based on the CBC mode of block cipher encryption. Basically, the construction is very similar to CBC-MAC, but the key is a public constant and the IV is a string of all zeros. Show that such a hash function is not CR2.

Problem 3 [20pts]

How does the cost of computing following operations compare with each other, when \( a_1, b_1, N_1 \) are all 1024-bit long, and \( a_2, b_2, N_2 \) are all 2048-bit long? Assume these are being performed on the same computer.

1. \((a_1+b_1) \mod N_1 \) and \((a_2+b_2) \mod N_2\)
2. \((a_1*b_1) \mod N_1 \) and \((a_2*b_2) \mod N_2\)
3. \((a_1^b_1) \mod N_1 \) and \((a_2^b_2) \mod N_2\)
4. \(\gcd(a_1,b_1) \) and \(\gcd(a_2,b_2)\)
5. \(a_1^{-1} \mod N_1 \) and \(a_2^{-1} \mod N_2\)

Problem 4 [15pts]

Argue why the following are true or false:
1. For x, y, a belonging to Z_N*, does x = 2y mod N \Rightarrow a^x = a^{2y} \mod N
2. For x, y, a belonging to 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 5 [15pts]**

1. Show why DDH is easy in 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 6 [15pts]**

2. What is the order of the group 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 7 [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 8 [20pts]**

1. In the class, we showed an attack breaking the IND-CCA2 property of El Gamal. Show why such an attack would not work for Cramer-Shoup encryption. (Note: don’t simply say that since Cramer-Shoup is IND-CCA2, no attack will work. Show why that particular attack, we described in the class for El Gamal, will not work for Cramer-Shoup)

**Problem 9 [10+10+5pts]**

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-bwww-cse.ucsd.edu/~mihir/papers/ro.pdf](http://www-bwww-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.