Mathematical Cryptology

Dept. of Information Technology
Lund University
Box 118, 221 00 Lund, Sweden

WEEK 2, 2013

Reading instructions:

- Chapter 9 (skip BAN logic part)
- Chapter 10
- Chapter 11

There will be 4 hours of lectures covering the above.

Hand-in exercises:

1) Review and Standard exercises: 9.1-9.3, 10.1-10.5, 11.1-11.13

2) Programming exercise: - (maximum 5 hours)

Hand in no later than **February 8, 2012.**

Ch 9: Review exercises:
9.1 Describe the key distribution problem.
9.2 How are nonces used in the protocols in this chapter?

Ch 9: Standard exercises:
9.3 Alice and Bob uses the following protocol for message distribution. Alice chooses her message M, a random value a and sends $A_1 = M \oplus a$. Bob then selects a random b and sends $B_1 = A_1 \oplus b$. Finally, Alice returns $A_2 = B_1 \oplus a$ to Bob. Bob can now compute the message as $A_2 \oplus b$. Show that this protocol is insecure as Eve can recover the message.

Ch 10: Review exercises:
10.1 What is a MAC? Give examples where one could use a MAC.
10.2 What is a suitable output size for a hash function?
10.3 What is the relation between the three different properties a hash function should meet?
10.4 Describe briefly how hash functions in the MD4 family are designed.

Ch 10: Standard exercises:
10.5 Give an example of a hash function that is preimage resistant but *not* second preimage resistant, assuming the existence of a preimage resistant hash function.

Ch 11: Review exercises:
11.1 What is the current fastest factoring algorithm?
11.2 What is meant by the problems FACTORING, RSA, QUADRES? Put the problems in order of difficulty.
11.3 What is meant by the problems DLP, DHP, DDH? Put the problems in order of difficulty.
11.4 Describe RSA encryption.
11.5 Could one ever have an RSA encryption exponent which was even?
11.6 Comment the statements:
a)Knowing RSA decryption exponent is equivalent to knowing the factors of the RSA modulus.
b) Breaking the RSA encryption algorithm is equivalent to factoring the RSA modulus.
11.7 ElGamal is a randomized encryption algorithms in that encrypting the same plaintext twice will produce different ciphertexts. Is this a good or bad property?
11.8 Describe advantages and disadvantages of Rabin encryption compared to RSA.

Ch 11: Standard exercises:
11.9 Let N denote an RSA exponent and let $\lambda(N) = \text{lcm}(p-1, q-1)$. If e is the encryption exponent, show that the decryption exponent d can be chosen so that

$$e \cdot d = 1 \pmod{\lambda)(N)}.$$

Hint: Show that $\lambda(N)$ is the largest order of an element in the group $\mathbb{Z}_N$.
11.10 Let N denote an RSA exponent and let $\lambda(N) = \text{lcm}(p-1, q-1)$. Suppose that the RSA encryption exponent e has order k in $\mathbb{Z}^*_{\lambda(N)}$. Show that

$$m^{e^k} = m \pmod{N}$$

. Hence conclude that the order of e modulo $p-1$ or $q-1$ should be large.
11.11 Show that if a user is stupid, and chooses a prime N as the modulus in the RSA scheme, it casn be trivially broken.

11.12 Explain why, for large plaintexts, it is better to use public key encryption to transport a symmetric key, and then to use a symmetric encryption scheme to encrypt the data.

11.13 Show that breaking the Rabin encryption algorithm is equivalent to factoring.