Mathematical Cryptology 2019

Dept. of EIT
Lund University
Box 118, 221 00 Lund, Sweden

WEEK 4,

Reading instructions:

- Chapter 13, 14 (partly repetition)
- Chapter 15

There will be 4 hours of lectures covering the above.

Hand-in exercises:

1) Review exercises: 13.1-13.7, 14.1-14.4

2) Standard exercises: 13.8-13.10, 14.5

3) Programming exercise:

Hand in no later than **February 26, 2019.**

Ch 13: Review exercises:
13.1 What is Kerchhoff's principle?
13.2 Describe the operation of a Feistel cipher.
13.3 What needs to change in a Feistel cipher between encryption and decryption?
13.4 Describe the operation of triple DES.
13.5 Describe the role of permutations and substitutions in DES.
13.6 Describe the role of permutations and substitutions in AES.
13.7 hat problems are associated with ECB mode, and how does CBC mode solve these issues?

Ch 13: Standard exercises
13.8 Let $\overline{a}$ denote the bitwise complement of a. Show that if

$$c = DES_k(m)$$

then

$$\overline{c} = DES_{\overline{k}}(\overline{m}).$$

13.9 Consider the following composition of a block cipher with an n-bit key size

$$c = E_{k_1}(E_{k_2}(m)),$$

to produce a cipher with a key size of $2n$ bits. Show that there is a chosen ciphertext attack on this composition that requires $O(2^n)$ memory and $O(2^n)$ encryptions/decryptions using E.

13.10 Consider triple DES but with two keys instead of three, i.e.,

$$c = DES_{k_1}(DES_{k_2}^{-1}(DES_{k_1}(m))).$$

Describe a chosen plaintext attack on this two-key version of triple DES, which requires roughly 2^{56} steps and storage of 2^{56} encryptions under single DES.

Ch 14: Review exercises:
14.1 What is a MAC? Give examples where one could use a MAC.
14.2 What is a suitable output size for a hash function?
14.3 What is the relation between the three different properties a hash function should meet?
14.4 Describe briefly how hash functions in the MD4 family are designed.

Ch 14: Standard exercises:
14.5 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 15: Review exercises:
15.1 What is the current fastest factoring algorithm?
15.2 What is meant by the problems FACTORING, RSA, QUADRES? Put the problems in order of difficulty.
15.3 What is meant by the problems DLP, DHP, DDH? Put the problems in order of difficulty.

15.4 Describe RSA encryption.
15.5 Could one ever have an RSA encryption exponent which was even?
15.6 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.

Ch 15: Standard exercises:
15.7 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

$$e \cdot d = 1 \bmod \lambda(N).$$

Hint: Show that $\lambda(N)$ is the largest order of an element in the group $\mathbb{Z}_N$.
15.8 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.
15.9 Show that if a user is stupid, and chooses a prime N as the modulus in the RSA scheme, it casn be trivially broken.
15.10 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.