Mathematical Cryptology, 2013

Dept. of EIT
Lund University

WEEK 1,

Reading instructions (online third edition of Smart's book):

- Appendix A (repetition)
- Chapter 1 (partly repetition)
- Chapter 3 (only repetition)
- Chapter 4 (only if you are interested)
- Chapter 5 (mostly repetition)
- Chapter 6 (only if you are interested)
- Chapter 7 (mostly repetition)
- Chapter 8 (partly repetition)

There will be 4 hours of lectures covering the above.

Hand-in exercises:

1) Review exercises: 1.1-1.9, 3.1-3.4, 5.1-5.5, 7.1, 8.1-8.9

2) Standard exercises: 1.10-1.13, 3.5, 8.10-12

3) Programming exercise: 1.14 (maximum 5 hours)

Hand in no later than **January 31, 2013.**

Ch 1: Review exercises:
1.1 What are the axioms of a group, ring and field?
1.2 Why are the nonzero integers not a group under multiplication?
1.3 Why do we say nonzero real numbers when we look at the reals as a group under multiplication?
1.4 Why are the integers not a field?
1.5 Why is $\mathbb{F}_p[x]/(f(x))$ always a ring?
1.6 What is the value of the Euler ϕ function at $N = p$ and $N = pq$, where p and q are primes.
1.7 Define the Legendre and explain how this is used to test for squares modulo a prime p.
1.8 If an integer a modulo a composite number N has Jacobi symbol 1 with respect to N, is it a square modulo N?
1.9 If there are 60 different coloured balls in a bag, how many do I have to take out on average (with replacement) before I obtain a repeated colour.

Ch 1: Standard exercises:
1.10 Show that if n is odd and factors in k distinct prime factors then the number of solutions of $x^2 = 1 \pmod{n}$ is equal to 2^k.
1.11 Show that g is a generator of $\mathbb{F}_p^*$ if and only if $g^{p-1} = 1 \pmod{p}$ and $g^{(p-1)/q} \neq 1 \pmod{p}$ for all prime divisors q of $p - 1$.
1.12 Given a composite integer N and the three integers $a, b, a^{1/3}b^{1/5} \pmod{N}$, show how you can compute $a^{1/3} \pmod{N}$ and $b^{1/5} \pmod{N}$ (with low complexity).
1.13 By hand or calculator, compute the Jacobi symbols

$$\left(\frac{311}{653}\right) \text{ and } \left(\frac{666}{777}\right).$$

Ch 1: Programming exercise:
1.14 Implement an algorithm to compute Legendre symbols which uses the law of quadratic reciprocity.

Ch 3: Review exercises:
3.1 What are the three most common letters in English? What are the most common bigrams and trigrams in English?
3.2 Explain how the Vigenére cipher is related to the shift cipher.
3.3 Explain relations between the substitution cipher and the Enigma cipher.
3.4 Describe the difference and similarities between permutation and substitution as cipher components.

Ch 3: Standard exercise:
3.5 In a chosen plaintext attack the attacker is allowed to ask for the encryption of a plaintext of her choosing. Show that the Caesar, Vigenére and substitution ciphers can be broken instantly under a chosen plaintext attack. Determine the smallest amount of plaintext needed.

Ch 5: Review exercises:
5.1 Is an attacker more interested in $p(C = c|P = m)$ or $p(P = m|C = c)$? Explain.
5.2 How is entropy defined?
5.3 If a random variable X takes at most t values, what are the maximum and minimum values possible for $H(X)$?
5.4 Are $H(P|K, C) = 0$ and/or $H(K, P) = H(K) + H(P)$ always true for any cipher? Explain why/why not.
5.5 Define the terms spurious keys and unicity distance.

Ch 7: Review exercises:
6.1 What is an LFSR? Whay can they not be used directly to create a stream cipher?

Ch 8: Review exercises:
8.1 What is Kerchhoff's principle?
8.2 Describe the operation of a Feistel cipher.
8.3 What needs to change in a Feistel cipher between encryption and decryption?
8.4 Describe the operation of triple DES.
8.6 Describe the role of permutations and substitutions in DES.
8.7 Describe the role of permutations and substitutions in AES.
8.8 hat problems are associated with ECB mode, and how does CBC mode solve these issues?
8.9 What is a MAC? Give example where one could use a MAC.

Ch 8: Standard exercises
8.10 Let $\overline{a}$ denote the bitwise complement of a. Show that if

$$c = DES_k(m)$$

then

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

8.11 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.

8.12 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.