Semester 1 **Exercises for Week 13** 2004

Review Tutorial

Let $\mathcal{A}$ be the alphabet $\{\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D}, \mathtt{E}\}$. Given the message `A BAD CAB A DEAD DAD`, we form the strip–encoded plaintext

$$M = \mathtt{ABADCABADEADDAD}$$

by removing all characters not in the alphabet.

1. Encipher the message M using the substitution key $K = \mathtt{BDEAC}$. Find the inverse key and verify the correctness by deciphering your ciphertext.

2. Let $\mathcal{A} \to \mathbb{Z}/5\mathbb{Z}$ be the bijection $\mathtt{A} \mapsto 0, \mathtt{B} \mapsto 1, \ldots, \mathtt{E} \mapsto 4$. Encipher the message M using the Vigenère key $K = \mathtt{ADECB}$ in ECB mode, then encipher the same message using the same key and initialization vector `BBBB`, in CFB and OFB modes with the block length $n = 5$ and $r = 1$. Rather than bit sum, use summation in $\mathbb{Z}/5\mathbb{Z}$ for the feedback. Verify the correctness of your results by then deciphering the ciphertext.

3. Let $K = [3, 5, 4, 1, 2]$ be a transposition key. Encipher the message M in ECB mode and in CBC mode. Verify the correctness of your results by deciphering the ciphertext.

4. Which of the modes of operation leaves Vigenère ciphertext open to attack by the Kasiski method? Which mode of operation was used for the block ciphers in the course assignments, and why?

Next we focus on some of the mathmematical problems which arise in stream ciphers and public key cryptography. The problems given are of a size which can be computed by hand, with minimal effort if the proper method is used.

Mathematics of LFSR's.

5. Let S be the set $\{x^6 + x + 1, x^6 + x^3 + 1, x^6 + x^5 + 1, x^6 + x^2 + 1\}$ of polynomials in $\mathbb{F}_2[x]$.
a. Which of the polynomials are irreducible?
b. Which of the polynomials are primitive?
c. What are the periods of the linear feedback shift registers with the above connections polynomials?
d. $(*)$ The polynomial $g(x) = x^6 + x^5 + x^4 + x^3 + 1$ is not irreducible. What is its factorization, and what are the periods of output sequence of a linear feedback shift register with $g(x)$ as connection polynomial and initial states 010011, 010010, and 111111?

Mathematics of RSA.

6. Let $G = (\mathbb{Z}/15\mathbb{Z})^*$.

a. What are the elements of G?

b. Show that $a = 2$ is a primitive element for $(\mathbb{Z}/3\mathbb{Z})^*$ and $a = 3$ is a primitive element for $(\mathbb{Z}/5\mathbb{Z})^*$.

c. Find an element a in $\mathbb{Z}$ which is primitive for both $(\mathbb{Z}/3\mathbb{Z})^*$ and $(\mathbb{Z}/5\mathbb{Z})^*$.

d. $(*)$ Why does it not make sense to speak of a primitive element for G?

e. $(*)$ How many elements a of G have the property of being primitive for both $(\mathbb{Z}/3\mathbb{Z})^*$ and $(\mathbb{Z}/5\mathbb{Z})^*$?

Mathematics of Diffie–Hellman.

7. Let $G_1 = (\mathbb{Z}/89\mathbb{Z})^*$ and $G_2 = (\mathbb{Z}/97\mathbb{Z})^*$.

a. Show that 7 is a primitive element for G_1 and for G_2.

b. Solve the discrete logarithm problem $\log_7(2)$ in G_1 and in G_2.

c. $(*)$ Which discrete logarithm is harder, and why?

Mathematics of Shamir's Secret Sharing Scheme.

Recall the Lagrange interpolation theorem:

Theorem 1 (Lagrange) *Let k be a field and let $f(x)$ be a polynomial over k of degree less than t. Given t distinct elements $x_1, x_2, \ldots, x_t$ of k, then $f(x)$ equals*

$$\sum_{i=1}^{t} f(x_i) \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{x - x_j}{x_i - x_j}$$

8. Let $\mathbb{F}_{31} = \mathbb{Z}/31\mathbb{Z}$ be the finite field of 31 elements, and let

$$\{(1,1), (2,16), (3,25), (4,28)\}$$

be a set of pairs of the form $(i, f(i))$ for some polynomial $f(x)$.

a. Find the value $f(0)$ of the polynomial $f(x)$ of degree 2 which interpolates the first three points.

b. Find the polynomial $f(x)$ of degree 2 which interpolates the first three points.

c. Show that the same polynomial passes through the fourth point.

d. Use the Lagrange interpolation theorem to conclude that $f(x)$ is the unique polynomial of degree less than 4 which passes through these four points.