Semester 1 **Exercises and Solutions 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.

Solution Recall that the key $K = \mathtt{BDEAC}$ specifies the map $\mathtt{A} \mapsto \mathtt{B}$, $\mathtt{B} \mapsto \mathtt{D}$, etc. This results in the enciphering

$$M = \mathtt{ABADCABADEADDAD} \mapsto C = \mathtt{BDBAEBDBACBAABD}.$$

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.

Solution We make the identification $M = \mathtt{ABADCABADEADDAD} = \mathtt{010320103403303}$ over $\mathbb{Z}/5\mathbb{Z}$. In the same way, we write $K = \mathtt{ADECB} = \mathtt{03421}$. The enciphering in ECB mode is then $\mathtt{044030440001223} = \mathtt{AEEADAEEAAABCCD}$. The enciphering in CBC mode begins with $C_0 = \mathtt{BBBBB} = \mathtt{11111}$, and since $E_K(C_{j-1} \oplus M_j) = C_{j-1} \oplus E_K(M_j)$, we just add in the previous ciphertext block to get

$$\mathtt{11111100141441410132} = \mathtt{BBBBBBAABEBEEBEBABDC}.$$

The application of this function E_K to form the state vectors I_j is particularly weak, since only the first character of the key K and the first character of the initialization vector. Since $K = \mathtt{A}****$, this means $I_j = \mathtt{B}****$, and so the ciphertext output is

$$\mathtt{BBBBBBCBEDBCBEABEEBE}.$$

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.

Solution The key $K = [3, 5, 4, 1, 2]$ specifies a transposition, under which $M \mapsto$ `ACDABAEDABDDAAD` in ECB mode. If we use the addition $\oplus$ of the previous question for the feedback, then we get ciphertext

`BBBBBACDABDADADCCAAC`.

Check this work carefully for errors – no guarantees.

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.

Solution We made use of the ECB mode in order to preserve the structure of a Vigenère ciphertext. This leaves this and other classical cryptosystems open to classical attacks such as the Kasiski method.

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?

Solution 1. 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.** The polynomials $x^6 + x + 1$, $x^6 + x^3 + 1$, and $x^6 + x^5 + 1$ are irreducible, but $x^6 + x^2 + 1 = (x^3 + x + 1)^2$.
- **b.** Of the three irreducible polynomials, we find that $x^6 + x^3 + 1$ generates LFSR output of period 9, so is not primitive. The other two irreducible polynomials generate output of period greater than $21 = 63/3$, so must be primitive.

c. The periods are therefore 63, 9, 63, and (at most) 14. The period of 14 can be determined for a specific value, but poor choices, like `1101001` can result in a period of 7, since the connection polynomial is not irreducible.

d. The polynomial $g(x) = x^6+x^5+x^4+x^3+1$ factors as $(x^2+x+1)(x^4+x+1)$. The LFSR outputs for initial states 010011, 010010, and 111111 with connection polynomial $g(x)$ are:

$$0100111001100000100111001100000 1\ldots$$
$$0100101010000110100101010000110 1\ldots$$
$$1111110001011101111100010111011\ldots$$

These each have periods 15, which equals $2^4 - 1$ (rather than $2^6 - 1$, which would be the case if $g(x)$ where irreducible.)

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 $(\mathbb{Z}/5\mathbb{Z})^*$?

Solution

a. The elements of $(\mathbb{Z}/15\mathbb{Z})^*$ are

$$\{1, 2, 4, 7, 8, 11, 13, 14\},$$

the elements of $\mathbb{Z}/15\mathbb{Z}$ coprime to 3 and 5.

b. Since $\{1, 2\} = (\mathbb{Z}/3\mathbb{Z})^*$ and $\{1, 3, 9 = 4, 27 = 2\} = (\mathbb{Z}/5\mathbb{Z})^*$, 2 and 3 are primitive elements for these moduli.

c. The integer 8 is primitive in $(\mathbb{Z}/3\mathbb{Z})^*$ and $(\mathbb{Z}/5\mathbb{Z})^*$, since 8 is a CRT lift of the pair $(2, 3)$ in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, i.e. $8 \equiv 2 \bmod 3$ and $8 \equiv 3 \bmod 5$.

d. There is no primitive element for $\mathbb{Z}/15\mathbb{Z}^*$ since no single element generates all of them. For instance the powers of 8 are:

$$1, 8, 64 = 4, 32 = 2, 16 = 1,$$

which generates a cycle of length only 4, whereas $(\mathbb{Z}/15\mathbb{Z})^*$ has eight elements.

e. The elements of $(\mathbb{Z}/15\mathbb{Z})^*$ which are primitive for both $(\mathbb{Z}/3\mathbb{Z})^*$ and $(\mathbb{Z}/5\mathbb{Z})^*$ are the two CRT images of the pairs $(2, 3)$ and $(2, 2)$.

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?

Solution

a. To show that 7 is a primitive element for $(\mathbb{Z}/89\mathbb{Z})^*$ and $(\mathbb{Z}/97\mathbb{Z})^*$, we need to show that

$$7^{44} \not\equiv 1 \bmod 89 \quad 7^{48} \not\equiv 1 \bmod 97$$
$$7^{8} \not\equiv 1 \bmod 89 \quad 7^{32} \not\equiv 1 \bmod 97$$

These values can be computed using products of successive squares of 7, e.g. $7^{44} = 7^4 7^8 7^{32}$, so $7^4 \equiv 87 \bmod 89$, $7^8 \equiv (-2)^2 \equiv 4 \bmod 89$, $7^{16} \equiv 16 \bmod 89$. Therefore $7^{44} \equiv -1 \bmod 89$, etc.

b. We find $\log_7(2) = 48$ in $\mathbb{F}_{89}$ and $\log_7(2) = 94$ in $\mathbb{F}_{97}$ using the baby-step, giant-step method.

c. A discrete logarithm in $(\mathbb{Z}/97\mathbb{Z})^*$ is theoretically easier to solve because $96 = 2^5 3$, so we solve the discrete logarithms using this factorization.

N.B. Verify that you can solve $\log_7(2)$ using $\log_{7^m}(2^m)$ where $m = 32$, and $m = 48, 24, 12, 6, 3$, and at each of the latter steps you only need to determine one additional bit of information.

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.

Solution 4. 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. The value $f(0)$ of the polynomial $f(x)$ of degree 2 which interpolates the first three points is given, using the first three shares, by

$$\begin{aligned} f(0) &= 1 \cdot \frac{(2)(3)}{(2-1)(3-1)} + 16 \cdot \frac{(1)(3)}{(1-2)(3-2)} + 25 \cdot \frac{(1)(2)}{(1-3)(2-3)} \\ &= 1 \cdot (3) + 16 \cdot (-3) + 25 \cdot (1) = 3 + 14 + 25 = 11. \end{aligned}$$

Using the last three shares we find:

$$\begin{aligned} f(0) &= 16 \cdot \frac{(3)(4)}{(3-2)(4-2)} + 25 \cdot \frac{(2)(4)}{(2-3)(4-3)} + 28 \cdot \frac{(2)(3)}{(2-4)(3-4)} \\ &= 16 \cdot (6) + 25 \cdot (-8) + 28 \cdot (3) = 3 + 17 + 22 = 11. \end{aligned}$$

N.B. Be careful to do any inversions modulo 31!!

b. Using the full formula, we get $f(x) = 28x^2 + 24x + 11$.

c. Verify: $f(4) = 28 \cdot 4^2 + 24 \cdot 4 + 11 = 14 + 3 + 11 = 28$.

d. Since the polynomial $f(x)$ agrees with the *four* points, this must be the unique polynomial of degree less than four which does so.