Queen Mary
University of London

MTH6115 Cryptography

Solutions 3

1 I use the following Latin square

	a	b	c	d
a	b	c	a	d
b	c	d	b	a
c	d	a	c	b
d	a	b	d	c

1) We have $a \oplus b = c$, $(a \oplus d) \oplus c = d$, $a \ominus c = a$.

2) The above Latin square gives the following ciphertext: `a bca bba cbdb cbc`.

3) Answer: `b ccc ddc bccb dbc`.

2 I will denote the (i, j)-entry of the Latin square by L_{ij}.

(i) The condition here is that if $a_i \oplus a_j = a_k$ then $a_k \oplus a_j = a_i$. (That is, if $L_{ij} = a_k$ then $L_{kj} = a_i$.) So the permutation corresponding to column a_j swaps a_i and a_k, and so squares to the identity (that is, has order 1 or 2). (We do allow $a_i = a_k$ in the above.)

(ii) The condition here is $L_{ji} = L_{ij}$ for all i and j.

(iii) A combination of the conditions in Parts (i) and (ii).

(iv) Already each column contains each symbol a_i exactly once. The symmetry of condition (ii), and thus (iii), now forces each row to contain each symbol exactly once, and so we have a Latin square.

(v) Such substitution tables exist for all n. One example is to take a substitution table on the integers modulo n in which $i \oplus j := -(i + j) \pmod{n}$. A similar construction works in any abelian group of order n.

(vi) For $n = 1, 2, 3, 4, 5$ there are $1, 2, 3, 16, 30$ such arrays respectively. Here are all the possibilities for $n \leqslant 3$.

	0
0	0

	0	1
0	0	1
1	1	0

	0	1
0	1	0
1	0	1

	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

	0	1	2
0	2	1	0
1	1	0	2
2	0	2	1

	0	1	2
0	2	0	1
1	1	2	0
2	0	1	2

Remark. Given a Latin square on $\mathscr{A}$ and a permutation σ on $\mathscr{A}$, we can form a new Latin square, which I call L^σ, by simultaneously permuting the rows and columns of $\mathscr{A}$ using σ. We regard the Latin squares L and L^σ as 'essentially equal'.

In the list above, the Latin squares with $n = 2$ are essentially equal, as are the latter two for $n = 3$, but the first one is different (because the number of i such that $i \oplus i = i$ is the same for two essentially equal squares). Finally, two squares of order 4, which are essentially different in the above sense, and two arrays of order 5, which must be essentially the same in my sense (no proof supplied here).

	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

	0	1	2	3
0	0	1	3	2
1	1	0	2	3
2	3	2	1	0
3	2	3	0	1

	0	1	2	3	4
0	0	4	3	2	1
1	4	3	2	1	0
2	3	2	1	0	4
3	2	1	0	4	3
4	1	0	4	3	2

	0	1	2	3	4
0	0	4	3	2	1
1	4	2	1	3	0
2	3	1	4	0	2
3	2	3	0	1	4
4	1	0	2	4	3

3 Notice that 11011 already appears in the above sequence (take the last three digits, then wrap around and take the first two). Accordingly, the output sequence generated from 11011 is the same is the one given, but you have to make a cyclic shift by 3, namely

[110111000010100].

Observe that we don't need to know the shift register itself to be able to do this. (But it is possible to recover the shift register from the given sequence.)

4 Each sequence has length 6, so in total they contain $6 + 6 = 12$ states. There are $2^4 - 1 = 15$ non-zero states, so the above sequences miss exactly three of them. By inspection, we see that 1101 does not appear in either of the sequences. The corresponding output sequence turns out to have period 3, namely it is [110]. What are the other two missing states?

5 For some polynomials the non-trivial cycles are as follows. Only the cycles are shown (without any extensions to confirm repetition), and they are to the right of any hyphens present. What is to the left of hyphens is the part of the sequence that does not repeat.

Polynomial	Factorisation	Lengths	Cycles
$x^4 + x + 1$	$x^4 + x + 1$	15	100010011010111
$x^4 + x^3 + 1$	$x^4 + x^3 + 1$	15	100011110101100
$x^4 + x^3 + x^2 + x + 1$	irreducible	$5, 5, 5$	$10001, 10010, 11110$
$x^4 + x^2 + 1$	$(x^2 + x + 1)^2$	$6, 6, 3$	$100010, 111100, 110$
$x^4 + x^2 + x$	$x(x^3 + x + 1)$	$1, 7$	a-0, a-1001011
$x^4 + x^3 + x$	$x(x^3 + x^2 + 1)$	$1, 7$	a-0, a-1001110
$x^4 + x^2$	$x^2(x + 1)^2$	$1, 1, 2$	ab-0, ab-1, ab-10
$x^4 + x^3 + x^2$	$x^2(x^2 + x + 1)$	$1, 3$	ab-0, ab-110
$x^4 + x^3$	$x^3(x + 1)$	$1, 1$	abc-0, abc-1
x^4	x^4	1	$abcd$-0

6 We determine the irreducible polynomials by ruling out all the factorizable ones. Note that a reducible polynomial of degree 6 must have an irreducible factor of degree at most 3 in its factorization. Here is the complete list of irreducible polynomials of degree at most 3:

$$x, \quad x+1, \quad x^2+x+1, \quad x^3+x+1 \quad \text{and} \quad x^3+x^2+1.$$

(The list is obtained by observing that an irreducible polynomial $f(x)$ of degree 2 or 3 can not be divisible by neither x nor $x+1$. So, $f(0) = f(1) = 1$ because we are working with binary coefficients. Writing out what this means in terms of coefficients of $f(x)$, we are left with the above list.) By throwing away all degree six polynomials that are divisible by one of the polynomials listed above, we will be left with all irreducible degree 6 polynomials.

The degree 6 polynomials $f(x) = x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ with a linear factor of x or $x+1$ satisfy $f(0) = 0$ or $f(1) = 0$. We throw these away and assume that $f(0) = f(1) = 1$. That is, $a_0 = 1$ and $1+a_5+a_4+a_3+a_2+a_1+a_0 = 1$, so $a_5 = 1 + a_4 + a_3 + a_2 + a_1$. We have 16 such polynomials.

Among these, to detremine those $f(x)$ that are divisible by $(x^2 + x + 1)$ we write $f(x) = q(x)(x^2 + x + 1)$ and vary $q(x)$ among degree 4 polynomials. We may assume that $q(x) = q(1) = 1$ (why?). Thus we find the four reducible polynomials given below:

$$x^6+x^3+x^2+x+1, \quad x^6+x^5+x^4+x^3+1, \quad x^6+x^5+x^3+x+1, \quad x^6+x^4+x^3+x^2+1.$$

Throwing away these fours, we are left with 12 polynomials. Among these 12 polynomials, we determine the ones that are products of two irreducible degree 3 polynomials. These are the following:

$$x^6 + x^2 + 1 = (x^3 + x + 1)^2, \quad x^6 + x^4 + 1 = (x^3 + x^2 + 1)^2$$
$$\text{and} \quad x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1).$$

Throwing away the above 3 polynomials, the 9 (as expected) remaining polynomials are therefore irreducible.

By writing out the output sequence of the corresponding shift register for each of the above 9 polynomials, we see that the following 6 are primitive:

$$x^6 + x + 1, \quad x^6 + x^4 + x^3 + x + 1, \quad x^6 + x^5 + x^2 + x + 1,$$
$$x^6 + x^5 + 1, \quad x^6 + x^5 + x^3 + x^2 + 1, \quad x^6 + x^5 + x^4 + x + 1.$$

The remaining 3, namely x^6+x^3+1, $x^6+x^4+x^2+x+1$ and $x^6+x^5+x^4+x^2+1$, give rise to shift registers with periods 9, 21 and 21 (if the initial state is not 000000). I leave the verification of this to you.

7 We take 5-bit sequences, and follow the sequence given by the shift register until we get repetition. Then take a 5-bit sequence you have not yet met, and repeat the process, until you get all 5-bit sequences. One should get something like the following (though you can vary the start points).

Period 21:	100001111101010011000-10000.
Period 7:	0010111-00101.
Period 3:	110-11011.

Here, the repeating parts, of lengths 21, 7 and 3 are shown before the hyphens, though one needs to go 5 beyond the hyphen to confirm repetition. The shift register does not have period $2^5 - 1$ for any 5-tuple, so it is not primitive. In fact, the polynomial is not irreducible, since $x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$ (with both factors irreducible).