MATHEMATICAL TRIPOS PART II (2023–2024)
CODING AND CRYPTOGRAPHY
EXAMPLE SHEET 4 OF 4

1 Show that, subject to a suitable non-degeneracy condition, any output stream $x_0, x_1, x_2, \ldots$ produced by a linear feedback shift register is *purely periodic*, i.e. there exists r such that $x_{n+r} = x_n$ for all $n \geq 0$.

2 A linear feedback shift register was used to generate the stream $110001110001\ldots$.

Recover the feedback polynomial by the Berlekamp-Massey method. (The LFSR has length 4 but you should work through the trials for length d for $1 \leqslant d \leqslant 4$.)

3 We work with streams of symbols in $\mathbb{F}_2$. I have a key sequence $k_1, k_2, \ldots$ and a message $p_1, p_2, \ldots, p_N$. I transmit $p_1 + k_1$, $p_2 + k_2$, $\ldots$, $p_N + k_N$ and then, by error, transmit $p_1 + k_2$, $p_2 + k_3$, $\ldots$, $p_N + k_{N+1}$. Assuming that you know this and that my message makes sense, how would you go about finding my message? Can you now decipher other messages sent using the same key sequence?

4 A non-linear feedback register of length 4 has defining relation $x_{n+1} = x_n x_{n-1} + x_{n-3}$. Show that the state space contains 4 cycles of lengths 1, 2, 4 and 9.

5 I announce that I shall be using the Rabin code with modulus N. My agent in X'Dofro sends me a message m (with $1 \leqslant m \leqslant N-1$) encoded in the requisite form. Unfortunately, my cat eats the piece of paper on which the prime factors of N are recorded so I am unable to decipher it. I therefore find a new pair of primes and announce that I shall be using the Rabin cipher with public modulus $N' > N$. My agent now recodes the message and sends it to me again.

The dreaded SNDO of X'Dofro intercept both code messages. Show that they can find m. Can they decipher any other messages sent to me using only one of the coding schemes?

6 (i) A user of RSA accidentally chooses a large prime for her modulus N. Explain why this system is not secure.

(ii) A popular choice for the RSA encryption exponent is $e = 65537$. Using this exponent how many multiplications are required to encrypt a message?

(iii) Show that if the primes p and q are chosen to be close then RSA is insecure. (By 'close' we mean $(p+q)/2$ is not much larger than $\sqrt{pq}$: we know that it is always at least as big).

7 Extend the Diffie-Hellman key exchange system to cover three participants in a way that is likely to be as secure as the two party scheme.

Extend the system to n parties in such a way that they can compute their common secret key in at most $n^2 - n$ communications of 'Diffie–Hellman type numbers'. The numbers p and g of our original Diffie-Hellman system are nown by everybody in advance.)

Show that this can be done using at most $2n - 2$ communications by including several 'Diffie–Hellman type numbers' in one message.

8 Recall the Elgamal signature scheme and briefly indicate how it defeats a homomorphism attack.

(i) Alice signs a sequence of messages, incrementing the value of k by 2 each time. Assuming Bob knows this, show that in most cases he can determine Alice's private key from two consecutive signed messages (without having to solve the discrete logarithm problem).

(ii) Suppose we drop the requirement that $1 \leqslant r \leqslant p-1$ from the Elgamal signature scheme. How might we then be able to forge signatures from old? [Hint: use the Chinese remainder theorem for the coprime moduli p and $p-1$.

9 Recall that if x_n is a stream which is periodic with period M and y_n is a stream which is periodic with period N then the streams $x_n + y_n$ and $x_n y_n$ are periodic with periods dividing the lowest common multiple of M and N. One of the most confidential German codes[1] involved a complex mechanism which the British found could be simulated by two loops of paper tape of length 1501 and 1497. If $k_n = x_n + y_n$ where x_n is a stream of period 1501 and y_n is a stream of period 1497, what is the longest possible period of k_n? How many consecutive values of k_n would you need to find the underlying linear feedback register using the Berlekamp–Massey method if you did not have the information given in the question? If you had all the information given in the question how many values of k_n would you need? [Hint: look at $x_{n+1497} - x_n$.]

You have shown that, given k_n for sufficiently many consecutive n we can find k_n for all n. Can you find x_n for all n?

10 Confident in the unbreakability of RSA, I write the following.

0000001 0000000 0002048 0000001 1391142

0000000 0177147 1033288 1391142 1174371

What mistakes have I made? Advise me on how to increase the security of messages.[2]

11 Let K be the finite field with 2^d elements. We recall that K^* is a cyclic group, generated by α say. Let $T : K \to \mathbb{F}_2$ be any non-zero $\mathbb{F}_2$-linear map.

(i) Show that the $\mathbb{F}_2$-bilinear form $S : K \times K \to \mathbb{F}_2$; $S(x, y) := T(xy)$ is non-degenerate (*i.e.* $T(xy) = 0$ for all $y \in K$ implies $x = 0$).

(ii) Show that the sequence $x_n = T(\alpha^n)$ is the output from a linear feedback shirt register of length at most d.

(iii) The period of $(x_n)_{n \geq 0}$ is the least integer $r \geqslant 1$ such that $x_{n+r} = x_n$ for all sufficiently large n. Show that the sequence in (ii) has period $2^d - 1$.

(

[1] codenamed FISH by the allies; this is because Bletchley Park had revealed that the Germans called their wireless teleprinter transmission systems 'Sägefisch' (sawfish). The marvellous tale of how FISH was broken is in Part 3 of the book 'Code Breakers: the inside story of Bletchley Park' edited by Harry Hinsley and Alan Stripp (OUP, 1993).

[2] This code is really no more sophisticated than the ones appearing in Edgar Allan Poe's *The Gold-Bug* or the Sherlock Holmes novel *The Adventure of the Dancing Men* by Arthur Conan Doyle.

12 Implement Shamir's (k, n)-threshold scheme (i.e. the 'secret sharing') of Chapter 20, taking $k = 2$, $n = 3$, $x_j = j + 1$, $p = 7$, $a_0 = S = 2$ and $a_1 = 3$. Check directly that any two people can find the secret S but that no single individual can.

Take $k = 3$, $n = 4$ and suppose that I foolishly try to implement Shamir's $(3, 4)$-threshold scheme by choosing $p = 6$. By considering systems of congruences mod 6, show that if I take $x_j = j$ then the first two members and the fourth member will be unable to determine a_0 uniquely, whereas if $x_j = j + 1$ then these members can determine a_0 uniquely.

Further Problem

13 Konstantin uses a one-time pad to communicate with the notorious spy Villanelle. The messages are coded in the obvious way, namely, if the pad has C, the third letter of the alphabet and the message has I, the ninth, then the encrypted message has L as the $(3+9)$th. We will work modulo 26. Unknown to them, the person whom they employ to carry the messages is actually the MI6 agent Eve in disguise. MI6 are on the verge of arresting Villanelle when Eve is given the message

$$LRPFOJQLCUD.$$

Eve knows that the actual message is

$$FLYXATXONCE,$$

and suggests that Q[3] 'changes things a little' so that Villanelle deciphers the message as

$$REMAINXHERE.$$

How will Q achieve this?

My final message to you:

```
klqhikg ip pl bawrqifre wp pmoikg
                                  gaowox jwkeat hlmcikp
```

[Hint: it is a substitution cipher.]

SM, Lent Term 2024
Comments on and corrections to this sheet may be emailed to `sm137@cam.ac.uk`

[3]Actually the character Q (code for Quartermaster) never appears in the novels by Ian Fleming, where Q and 'Q Branch' are merely mentioned. Charles Fraser-Smith is widely credited as the inspiration for Q, for which see the New Scientist article 'Careful Carruthers That Paper Clip Is Loaded' from August 1993.