MATHEMATICAL TRIPOS PART II (2006–07)

Coding and Cryptography - Example Sheet 4 of 4 **T.A. Fisher**

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

47) 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 $1 \leq d \leq 4$.)

48) We model English text by a sequence of random variables $(X_n)_{n\geq 1}$ taking values in $\Sigma = \{A, B, \ldots, Z, \texttt{space}\}$. The entropy of English is $H_E = \lim_{n\to\infty} H(X_1, \ldots, X_n)/n$.
(a) Assuming H_E exists, show that $0 \leq H_E \leq \log 27$.
(b) Taking $H_E \approx \log 3 \approx 1.58$, estimate the unicity distance of (i) the substitution cipher, and (ii) the Vigenère cipher.

49) 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?

50) 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.

51) I announce that I shall be using the Rabin code with modulus N. My agent in X'Dofro sends me a message m (with $1 \leq m \leq N-1$) 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 code with 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?

52) (i) A user of RSA accidentally chooses a large prime for his 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) Why might it be a bad idea to use an RSA modulus $N = pq$ with $|p - q|$ small?

53) Alice and Bob are issued with RSA public keys (N, e_1) and (N, e_2), and corresponding private keys (N, d_1) and (N, d_2).
(i) The same message m is sent to both Alice and Bob. Assuming e_1 and e_2 are coprime, how can we recover m from the intercepted cipher texts c_1 and c_2?
(ii) How can Alice read messages sent to Bob?

54) 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.

55) Recall the ElGamal signature scheme and briefly indicate how it defeats a homomorphism attack. Alice signs a sequence of messages, incrementing the value of k by 2 each time. How can Bob determine Alice's private key from any two consecutive signed messages (without having to solve the discrete logarithm problem)?

Further Problems

Note: the examples above are minimal to cover the course; you are encouraged to do those below also.

56) (i) Suppose that x_n is a stream which is periodic with period M and y_n is a stream which is periodic with period N. Show that the streams $x_n + y_n$ and $x_n y_n$ are periodic with periods dividing the lowest common multiple of M and N.
(ii) One of the most confidential German codes (called FISH by the British) 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 stream of period 1497, what is the longest possible period of k_n? How many consecutive values of k_n do you need to specify the sequence completely?

57) Criticise the following authentication procedure. Alice chooses public key N for the Rabin cryptosystem. To be sure we are in communication with Alice we send her a "random item" $r = m^2 \pmod N$. On receiving r, Alice proceeds to decode using her knowledge of the factorisation of N, and finds a square root m_1 of r. She returns m_1 to us and we check that $r = m_1^2 \pmod N$. (You should think about what happens when many mutually distrusting parties communicate with Alice in this way.)

58) 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 $K \times K \to \mathbb{F}_2$; $(x, y) \mapsto T(xy)$ 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 LFSR of length d.
(iii) The period of $(x_n)_{n \geq 0}$ is the least integer $r \geq 1$ such that $x_{n+r} = x_n$ for all sufficiently large n. Show that the sequence in (ii) has period $2^d - 1$.

59) Suppose we drop the requirement $1 \leq r \leq p - 1$ from the ElGamal signature scheme. How might we then be able to forge new signatures from old? (Hint: Use the Chinese Remainder Theorem for the coprime moduli p and $p - 1$.)

60) We use RSA with public key (N, e) and private key (N, d). Suppose that $N = pq$ where p and q are primes with the same number of binary digits.
(i) Show that $N - \phi(N) < 3\sqrt{N}$.
(ii) Let $k = (de - 1)/\phi(N)$. Show that k is an integer less than d.
(iii) Show that if $d < \frac{1}{3} N^{1/4}$ then

$$\left| \frac{k}{d} - \frac{e}{N} \right| < \frac{1}{3d^2}.$$

(iv) It is known that if x is a positive real number and a, b are integers with

$$\left| x - \frac{a}{b} \right| < \frac{1}{2b^2}$$

then a/b arises from the continued fraction expansion of x. Explain how this observation may be used to attack RSA.