MATHEMATICAL TRIPOS PART II (2004–05)

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

61) We work with streams of symbols in $\mathbb{F}_2$. I have a secret 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 part of my secret sequence?

62) 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 to specify the sequence completely?

63) 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 necessarily periodic, i.e. there exists N such that $x_{r+N} = x_r$ for all $r \geq 0$.

64) Prove that if a linear feedback shift register has maximum period then this period may be achieved by any non-zero initial vector. Give an example of a register of length 4 with this property.

65) A binary 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.

66) I announce that I shall be using the Rabin-Williams scheme 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 Williams scheme 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?

67) The modulus $N = 713$ is used for the Rabin-Williams code. The ciphertext received is $c = 289$. Determine all possible plaintexts.

68) A user of RSA accidently chooses a large prime for his modulus N. Explain why this system is not secure.

69) Suppose that A and B use RSA with public keys (N, e_1) and (N, e_2) where e_1 and e_2 are coprime. The same message m is sent to both A and B. How can we recover m from the intercepted ciphertexts c_1 and c_2?

70) How many multiplications are needed for RSA encryption with exponent $e = 65537$?

71) (i) Describe an efficient method for checking that 3 is a primitive root mod 89.
(ii) Use the Baby-Step Giant-Step algorithm to solve the discrete logarithm problem $3^x \equiv 19 \pmod{89}$. [The sequence $19.3^{-n} \pmod{89}$ begins 19, 36, 12, 4, 31, 40, 43, 44, 74. The sequence $3^{10n} \pmod{89}$ begins 1, 42, 73, 40, 78, 72, 87, 5, 32.]

72) 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. (The numbers p and g of our original Diffie-Hellman system are known by everybody in advance.)

73) Give an example of a homomorphism attack on an RSA code. Show in reasonable detail that the el Gamal signature scheme (even without the use of a hash function) defeats it.

74) Suppose we drop the requirement $1 \leq r \leq p-1$ from the el Gamal signature scheme. How might we then be able to forge new signatures from old?

Further Problems

The following problems are not intended to be any harder than those earlier on the sheet.

75) Show that if we accept as true the emperical evidence that any ciphertext of 40 or more symbols from the 26-letter alphabet can be uniquely deciphered into meaningful plaintext by a substitution cipher, then the entropy of English is ≤ 2.5 bits/symbol.

76) Prove that for any source (no matter how correlated) if the message is encrypted using a one-time pad, then the symbols of the ciphertext are uniformly distributed and independent.

77) Let $N = pq$ be a product of odd distinct primes. Show that $x^2 \equiv d \pmod{N}$ can have 0, 1, 2 or 4 solutions depending on d. Give examples to show that each of these possibilities can occur.

78) Criticise the following authentication procedure. Alice chooses public key N for the Rabin-Williams code. 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 or 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.]

79) Why might it be a bad idea for all users of a public key system based on RSA to use the same modulus N (but different exponents d and e)?

80) Alice and Bob carry out a Diffie-Hellman key exchange with $p = 29$ and $g = 2$. If the numbers exchanged by Alice and Bob are 9 and 12, what is their secret key?