Question 1 (a) Which method gives ciphers that are harder to break: 1) an affine substitution composed with another affine substitution; 2) a Caesar shift composed with an affine substitution then composed with another Caesar shift. Justify your answer. [4]

(b) The following cipher text has been encrypted using the affine substitution $\theta_{5,4}$:

$$QAMMYL\ JLYEC.$$

Decrypt it. [6]

(c) How many affine substitutions are there on an alphabet of size 60? How many Vigenère keys of length 10 are there on this alphabet? [6]

Solution:

(a) Both of them amount to affine ciphers, so they have equal difficulty.

(b) First find the inverse $\theta_{a,b}$ by solving

$$\begin{cases} 5a \equiv 1 & \pmod{26} \\ 4a+b \equiv 0 & \pmod{26} \end{cases}$$

The solution is $a \equiv -5 \pmod{26}$ and $b \equiv -6 \pmod{26}$. Applying $\theta_{-5,-6}$ to the ciphertext we find the plain text to be *summer break*.

(c) There are $60\phi(60) = (60)(2)(2-1)(3-1)(5-1) = 960$ affine cipher. There are 60^{10} Vigenère keys of length 10.

Question 2 (a) Define what a stream cipher on a given alphabet is, explaining all its ingredients. Explain what the advanteges of a one-time pad over a Vigenère cipher are. [8]

(b) Consider the following two substitution tables on the three letter alphabet $\{a,b,c\}$:

	a	b	c
a	a	a	b
b	c	b	a
c	b	c	c

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Suppose you want to create a secure stream cipher. Which one would you use? Justify your answer. [3]

(c) Suppose you intercepted the ciphertext

$$abbccc$$

and you have reason to believe that it has been encrypted using the left table in part (b). Suppose you also know that the key is

$$cabbac$$

Decrypt the message. [5]

Solution:

(a) A stream cipher on an alphabet A of size n is given by a substitution table and a key of the same length as the plaintext. A substitution table means an $n \times n$ square matrix whose rows and columns are indexed by elements of A and whose entries are elements of A. We require that there are no repetitions in the columns . This gives rise to a binary operation $\oplus$ which is used to define the encryption function:

$$plaintext \oplus key = ciphertext.$$

The advantages of a one-time pad over the Vigenère cipher are: 1) the key is a random sequence as opposed to the periodic keys of Vigenère; 2) we can choose alternative Latin squares instead of the Vigenère square.

(b) The square on the right is a Latin square, so by Shannon's theorem it can be used to produce an unbreakable cipher.

(c) By subtracting the key from the ciphertext we find the plaintext to be *bcbcbc*. (points for knowing what subtraction means, and points for the correct answer.)

Question 3 (a) Define the Euler function $\phi(n)$ and the Carmichael function $\lambda(n)$. Evaluate $\lambda(55)$. [5]

(b) Let n be an odd number such that $\phi(n) = \lambda(n)$. Prove that there is a prime number p such that $n = p^r$ for some integer $r \geq 1$. [6]

(c) Show how RSA with modulus N can be broken if $\lambda(N)$ is known. Illustrate this by factorizing 589, given that it is a product of two primes and $\lambda(589) = 90$. (The marks are for the method, not the factorisation.) [7]

Solution:

(a) The Euler function $\phi(n)$ is the number of congruence classes mod n that are coprime to n. The Carmichael function $\lambda(n)$ is the smallest number m such that $x^m \equiv 1 \pmod{n}$ for all x coprime to n. We have $\lambda(55) = lcm\{5-1, 11-1\} = 20$.

(b) Let $n = p_1^{r_1} \cdots p_k^{r_k}$ be the prime factorisation of n. Then we have $\phi(n) = \phi(p_1^{r_1}) \cdots \phi(p_k^{r_k})$ while $\lambda(n) = lcm\{\phi(p_1^{r_1}), \cdots, \phi(p_k^{r_k})\}$. Since $\phi(p_i^{r_i})$ are all even, the only case where the two sides can be equal is when $k = 1$.

(c) First we find r, the residue of division of $N = 589$ by $2\lambda(N) = 180$. The answer is 49. Then we solve $x^2 - (r+1)x + N = x^2 - 50x + 589 = 0$. . The roots are the prime factors of 589: 31 and 19.

Question 4 (a) Define what it means for a binary n-bit shift register to be primitive. Give an example of a primitive binary 3-bit shift register. Justify your answer. [5]

(b) The following is the first 10 digits in the output sequence of a binary 5-bit shift register:

0011110110.

Determine the rest of the sequence and its period. [8]

(c) Is this shift register primitive? Is the periodic part of the sequence you obtain in part (b) pseudo-noise? Justify your answers. [5]

Solution:

(a) A primary n-bit shift register is one whose output sequence (for some, equivalently any, initial state) contains every possible nonzero binary sequence of length n. (Alternative definition: the output sequence has period $2^n - 1$.)

A binary polynomial of degree 3 is irreducible if and only if it has no linear factor, i.e., $f(0)$ and $f(1)$ are non-zero. By inspection we see that there are exactly two such polynomials: $f(x) = x^3 + x^2 + 1$ and $f(x) = x^3 + x + 1$. Either by verifying the output sequence, or using the formula $\frac{1}{3}\phi(2^3 - 1)$, we see that both are primitive.

(b) First we determine the shift register by solving the equations

$$\begin{cases} a_2 + a_3 + a_4 &= 1 \\ a_1 + a_2 + a_3 + a_4 &= 0 \\ a_0 + a_1 + a_2 + a_3 &= 1 \\ a_0 + a_1 + a_2 + a_4 &= 1 \\ a_0 + a_1 + a_3 + a_4 &= 0 \end{cases}$$

The solution is $a_0 = 1$, $a_1 = 1$, $a_2 = 1$, $a_3 = 0$, and $a_4 = 0$. Having determined the shift register, we take the last 5 digits of our sequence as the input, and generate the rest of the sequence. The complete output has period 14. The repeating part is 00111101100001.

(c) The shift register is not primitive as its period is smaller than $31 = 2^5 - 1$. The sequence fails Golomb's postulates (G2) and (G3). For example, the number of runs of length 1,2,3 and 4 are 2,2,0 and 2, respectively.

Question 5 (a) Explain how the Diffie-Hellman key exchange is implemented in the RSA cryptosystem. [6]

(b) What is the knapsack problem? What is known about the complexity of the knapsack problem? [4]

(c) Suppose Alice and Bob are using the knapsack cipher and that Bob's key is

$$(22, 2, 46, 5, 100, 1, 702, 10, 351).$$

Alice sends the message 1088 to Bob. Decipher it (write your answer in the form of a binary sequence). [5]

Solution:

(a) Assume that Alice wants to send a secret message to Bob. Alice and Bob agree on a modulus p, a prime number. They must share the prime p, so they must assume that Eve knows it. Each of them chooses a number coprime to $\lambda(p) = p-1$, and computes its inverse. These numbers are not revealed. Alice chooses d_A and e_A, Bob chooses d_B and e_B. Let T_d be the map $x \mapsto x^d \pmod p$. Note that the commutation condition is satisfied:

$$T_{d_A} T_{d_B}(x) = x^{d_A d_B} \pmod p = T_{d_B} T_{d_A}(x).$$

Now Alice takes the message x and applies T_{e_A}; she sends $T_{e_A}(x)$ to Bob. Bob applies T_{e_B} and returns $T_{e_B} T_{e_A}(x)$ to Alice. Alice applies T_{d_A} and returns

$$T_{d_A} T_{e_B} T_{e_A}(x) = T_{d_A} T_{e_A} T_{e_B}(x) = T_{e_B}(x)$$

to Bob, who then applies T_{d_B} and recovers $T_{d_B} T_{e_B}(x) = x$, the original message.

(b) Given positive integers $a_1, \cdots, a_k$ and another positive integer b, the knapsack problem is to write b as a sum of some of the a_i, or show that this is impossible. It is known to be an NP-complete problem.

(c) Arranged in the increasing order, these number form a super-increasing sequence, so we can use Greedy algorithm. We find

$$1088 = (1)22 + (1)2 + (0)(46) + (0)5 + (0)100 + (1)1 + (1)702 + (1)10 + (1)351.$$

So the message is 110001111.

Question 6 (a) Explain the operation of the El-Gamal cipher for encrypting messages. Which hard problem is it based on? [5]

(b) Why is it important that in Bob's El-Gamal public key (p, g, h) the number g is a primitive root mod p? Is $(97, 8, 33)$ a suitable El-Gamal public key? Justify your answer. [5]

(c) Bob's El-Gamal public key is $(83,5,52)$ and his secret key is $a = 9$. Bob receives the message $(2,40)$ from Alice. Decipher it, simplifying your answer as much as possible. [7]

Solution:

(a) Bob's public key is (p,g,h) where p is prime, g is a primitive root mod p and $h = g^a$, where $1 \leq a \leq p-2$ is Bob's secret key. To send a message $1 \leq x \leq p-1$ to Bob Alice chooses a random $1 \leq k \leq p-1$ and sends the pair (g^k, xh^k) to Bob. El-Gamal is based on the discrete logarithm problem.

(b) To break El-Gamal, it is enough to determine the secret key a by solving the equation $g^a \equiv h \pmod{p}$. When g has a small order, this is easy to solve. Therefore we need to make sure that g has the maximum order possible, i.e., is primitive. This is not a suitable El-Gamal key because $8 = 2^3$ is not a primitive root mod 97; we have, by Fermat, $8^{32} = 2^{96} \equiv 1 \pmod{97}$. (In fact, the order of 8 modulo 97 is 16.)

(c) The plaintext is $(2^9)^{-1}(40) \pmod{83}$. We have

$$2^9 \equiv (128)(4) \equiv (45)(4) \equiv 14 \pmod{83}.$$

So $(2^9)^{-1} \equiv 6 \pmod{83}$. Thus, the message is $(6)(40) = 240 \equiv 74 \pmod{83}$.

