Problem 1. (20 points)
We recall that one-time pad (OTP) encryption consists of adding a random key of the same size as the plain text to a plain text message. This results in a random cipher text. For a message of size n and an alphabet of cardinality m we have

$$e(m_1, \ldots, m_n) = c_1, \ldots, c_n \text{ with } c_i \equiv m_i + k_i (\text{mod } m)$$

and

$$d(c_1, \ldots, c_n) = m_1, \ldots, m_n \text{ with } m_i \equiv c_i - k_i (\text{mod } m).$$

(a) One of the following two strings has been encrypted using a simple substitution cipher and the other with OTP. Determine the type of encryption by computing the index of coincidence and explain your answer. We consider the roman alphabet of size 26 and english language.

$s_1 =$	rczbw	bfhsl	pscpi	lhbgz	jtgbi	bjgly	ijibf	hcqqf	zbyfp
$s_2 =$	khqwg	izmgk	poyrk	huitd	uxlxc	wzotw	pahfo	hmgfe	vuejj

In the following we consider a binary alphabet ($m = 2$). OTP is equivalent to

$$c_i = m_i \oplus k_i \text{ and } m_i = c_i \oplus k_i$$

where $\oplus$ is the binary XOR operation. $\{0,1\}^n$ denotes the set of all binary strings of length n. It is known that OTP encryption has perfect secrecy if $\mathcal{M} = \mathcal{K} = \{0,1\}^n$ and the key $k = k_1, \ldots, k_n$ is uniformly distributed. Now we want to consider variations of OTP with restrictions on the plaintext and the key. In particular, the set $S = \{00, 01, 10\}$ is considered.
Consider the following three OTP variants where the key is always chosen uniformly at random:

1. Let $\mathcal{M} = S^n$ and $\mathcal{K} = \{0,1\}^{2n}$. In this way, both the message and the key are bit strings of length $2n$, but not every bit string of length $2n$ can be a valid message. For example, for $n = 3$, we could have $m = 00, 01, 00$ but not $m = 11, 00, 11$ because $11 \notin S$.
2. Let $\mathcal{M} = \{0,1\}^{2n}$ and $\mathcal{K} = S^n$.
3. Let $\mathcal{M} = \mathcal{K} = S^n$.

For each of these OTP variants answer following questions:

(b) What are the sizes of the message space $\mathcal{M}$ and the key space $\mathcal{K}$.

(c) Determine the space $\mathcal{C}$ of the ciphertexts.

(d) Has the resulting cipher perfect secrecy? Explain your answer.

(e) In which way is the size of the key space and the message space related to the property of perfect secrecy? Explain how and why.

Problem 2. (20 points)
Alice and Bob want to use the number $p = 1373$ and the base $a = 2$ for a Diffie-Hellman key exchange.

(a) Use the Miller-Rabin test to show that 2 is not a strong witness for the compositness of p.

(b) Which condition must be fulfiled by a to be feasible for the Diffie-Hellman key exchange protocol? Check if a actually fulfils this condition (Hint: $2^{196} \equiv 333 (\text{mod } 1373)$).

Alice sends $u = 974$ to Bob.

(c) Given that Bob's secret is 871, compute the shared key.

The Diffie-Hellman key exchange is based on the Diffie-Hellman problem. A variant of this problem is the Diffie-Hellman Decision problem. It is stated as follows. Given three numbers u, v and w with

$$u \equiv a^x (\text{mod } p) \text{ and } v \equiv a^y (\text{mod } p),$$

determine wether

$$w \equiv a^{xy} (\text{mod } p)$$

(d) Prove that an algorithm that solves the Diffie-Hellman problem can be used to solve the Diffie-Hellman Decision problem.

Problem 3. (20 points)
Alice uses the RSA algorithm and encrypts a message m with Bob's public key $(n, e) = (91, 59)$.

(a) Find the plaintext associated with the ciphertext $c = 23$. Write down all steps of your calculations.

Now imagine Alice wants to send the same message x to three different people Bob, Bart and Barney. Each of them uses the same public encryption exponent $e = 3$. Let their public moduli be n_1, n_2 and n_3, respectively. Alice thus sends to each of them $c_i \equiv x^3 (\text{mod } n_i)$.

(b) First let us assume that at least two public moduli n_i are **not** relatively prime (for example $\gcd(n_1, n_2) \neq 1$). How can you find x given all c_i's?

(c) Second, assume that $n_1 = 46$, $n_2 = 51$ and $n_3 = 77$ and $c_1 = 31$, $c_2 = 19$ and $c_3 = 71$. We have

$$\begin{aligned} 31 &\equiv x^3 (\text{mod } 46) \\ 19 &\equiv x^3 (\text{mod } 51) \\ 71 &\equiv x^3 (\text{mod } 77) \end{aligned}$$

Compute x, given all c_i's (and the public information) without factoring any of the moduli.

(d) Oscar can only intercept the first two ciphertexts. Is it possible to decrypt the ciphertext from the first two congruences (without factoring any of the moduli)?

$$\begin{aligned} 31 &\equiv x^3 (\text{mod } 46) \\ 19 &\equiv x^3 (\text{mod } 51) \end{aligned}$$