Victer Phiathep
Cryptography & Comp Sec
Theoretical Assignment 1

1.1 : For a Vigenere key of length 4, there are 26 possible letters for each position in the key, giving a total of 26^4 possible keys. However, the last string must be of size 2 to get to 26, so we need to adjust for this. There are 26 possible letters for the first three positions in the key, and 26*26 = 676 possible combinations for the last two positions in the key. Therefore, the total number of different Vigenere keys of length 4 that can be used to encode the English alphabet is:

26^3 * 676
= 17,576,576

1.2: $(2^8)^{n/8}$

1.3 In a known plaintext attack, the attacker has access to pairs of plaintext-ciphertext messages and can use this information to discover the key r.

Let's consider a pair of plaintext-ciphertext messages (P, C), where P is the plaintext and C is the corresponding ciphertext. We know that the ciphertext is obtained by XORing the plaintext with the random key r:

C = P XOR r

If we XOR the ciphertext with the plaintext, we obtain:

C XOR P = (P XOR r) XOR P = r

Therefore, by XORing the plaintext and ciphertext, we can recover the key r. This is possible because the XOR operation is reversible - if we XOR two values and the result, we can recover the missing value.

2.1: Let's consider a number n that ends with the digit 1. This means that n can be written as:
n = 10k + 1
where k is an integer.
Now, let's consider the powers of n. The first few powers of n are:

n^1 = 10k + 1
n^2 = (10k + 1)^2 = 100k^2 + 20k + 1 = 10(10k^2 + 2k) + 1
n^3 = (10k + 1)^3 = 1000k^3 + 300k^2 + 30k + 1 = 10(100k^3 + 30k^2 + 3k) + 1
n^4 = (10k + 1)^4 = 10000k^4 + 4000k^3 + 600k^2 + 40k + 1 = 10(1000k^4 + 400k^3 + 60k^2 + 4k) + 1

We can see that in each power of n, the term 10k appears in front of the final digit 1. Therefore, the final digit of each power of n will be 1, since the term 10k does not affect the final digit.

2.2: Let's consider a number n that ends with the digit 9. This means that n can be written as:
n = 10k + 9
where k is an integer.

If we square n:
n^2 = (10k + 9)^2 = 100k^2 + 180k + 81

We can rewrite this expression as:
n^2 = 100k^2 + 180k + 80 + 1

Notice that the first three terms are divisible by 10 and therefore end with 0. The last term is 1 because 9 times 9 is 81. Therefore, we can simplify the expression as:
n^2 = 10(10k^2 + 18k + 8) + 1

Since the first term, 10(10k^2 + 18k + 8), is divisible by 10, it does not affect the final digit of the expression. Therefore, the final digit of n^2 is 1.

2.3: To show that 1001^978 - 3429^2 is divisible by 10, we need to show that the difference is a multiple of 10.

We can do this by checking if the last digit of the difference is 0. If the last digit is 0, then the number is divisible by 10. To find the last digit of the difference, we can first simplify the expressions by considering the last digits of the two numbers. The last digit of 1001 is 1, and the last digit of 3429 is 9. Therefore, the last digit of 1001^978 will always be 1, and the last digit of 3429^2 will always be 1.

So, we can write:
1001^978 - 3429^2 = (1000 + 1)^978 - 3429^2
= 1000^978 + 978*1000^977 + ... + 1 - 3429^2

The last digit of 1000^978 is 0, since any power of 10 will end in 0. Also, the last digit of 3429^2 is 1.

So, we can simplify the expression further by ignoring all terms except the last two:
1001^978 - 3429^2 = ... + 1 - 1 = 0

Therefore, the last digit of the difference is 0, which means that 1001^978 - 3429^2 is divisible by 10.

3.1:
For a = 112 and b = 32, we have:
112 = 3 × 32 + 16
32 = 2 × 16 + 0

Therefore, the GCD of 112 and 32 is 16.

For a = 114 and b = 68, we have:
114 = 1 × 68 + 46
68 = 1 × 46 + 22
46 = 2 × 22 + 2
22 = 11 × 2 + 0

Therefore, the GCD of 114 and 68 is 2.

4. Using the extended Euclidean algorithm, we can find x and y:

First, we set up the table:

i	ri	si	ti
0	112	1	0
1	32	0	1

Then we use the following formulas to compute each row:

ri = ri-2 - q * ri-1
si = si-2 - q * si-1
ti = ti-2 - q * ti-1

where q is the quotient of ri-2 divided by ri-1.

Applying these formulas, we get:

i	ri	si	ti
0	112	1	0
1	32	0	1
2	16	1	-3
3	0	-3	10

Therefore, we have x = 1 and y = -3, so:

1 * 112 + (-3) * 32 = 16

For the second example, a = 114 and b = 68, we have already determined that the GCD is 2. Using the extended Euclidean algorithm, we can find x and y:

Setting up the table, we get:

i	ri	si	ti
0	114	1	0
1	68	0	1
2	46	1	-1
3	22	-1	2
4	2	6	-11
5	0	-23	42

Therefore, we have x = 6 and y = -11, so:

6 * 114 + (-11) * 68 = 2

5.

To solve the modular equation 9x ≡ 15 (mod 30), we need to find all values of x that satisfy the equation.

First, we can simplify the equation by dividing both sides by the greatest common divisor of 9 and 30, which is 3:
9x ≡ 15 (mod 30)
3x ≡ 5 (mod 10)

Now we need to find the inverse of 3 modulo 10. This means we need to find an integer y such that:
3y ≡ 1 (mod 10)

We can use the extended Euclidean algorithm to find y:

i	ri	si	ti
0	10	0	1
1	3	1	0
2	1	-3	1
3	0	10	-3

So, we have y = -3, which means:
3(-3) ≡ 1 (mod 10)
-9 ≡ 1 (mod 10)
1 ≡ -9 (mod 10)

Therefore, we can multiply both sides of the simplified equation by y = -3:
3x ≡ 5 (mod 10)
-9x ≡ -15 (mod 10)
x ≡ 5 (mod 10)

So the solutions to the modular equation are given by:
x ≡ 5 (mod 10)

This means that all solutions can be written in the form x = 5 + 10k, where k is any integer.