Question 1.

(a) ASCII characters. Original message is HALF OF A POINT IS YOURS, including space characters.

(b) Morse code. 'e' is '.', 'm' is '-' (long syllable). Message is NEW YORK.

(c) Anagram. MINOTAUR or MAIN TOUR.

(d) Binary system transformed into decimal one, get the alphabet characters according to their alphabet order, A=1. NORTH TOWER.

(e) Order of prime numbers, get alphabet characters according to this order. YETTI FOUND.

(f) Caesar cipher, shift = 8 to the right. ATTACK AFTER DINNER.

(g) Atbash cipher. KING IN AVIGNON.

(h) Scytale cipher, 4 letters around the circle. FOLLOW THE MAN IN BLACK.

Question 2.

(a) (i) Using $e_{a,b}(x) = a*x+b(mod26)$, where x is each letter of word CODING, we get numbers 12,14,23,0,3,4. That gives us cryptotext MOXADE.

(ii) Using $d_{a,b}(x) = (x-b)*a^{-1}(mod26)$, where x is each letter of cryptotext MVUZRO, we obtain numbers 2,17,24,19,14,15. That gives us encrypted word CRYPTO.

(b) (i) Encrypting "CODING", corresponding numbers are 2,14,3,8,13,6, operations mod 26.

$$M * \begin{bmatrix} 2 \\ 14 \\ 3 \end{bmatrix} = \begin{bmatrix} 25 \\ 3 \\ 4 \end{bmatrix}; M * \begin{bmatrix} 8 \\ 13 \\ 6 \end{bmatrix} = \begin{bmatrix} 9 \\ 0 \\ 7 \end{bmatrix}$$

We see that we get numbers 25,3,4,9,0,7 so encrypted word is ZDEJAH.

(ii) Corresponding numbers for JTUYVC are 9,19,20,24,21,2. For decoding we need to find M^{-1} in mod 26.

$$M^{-1} = \begin{bmatrix} 9 & 25 & 23 \\ 2 & 10 & 3 \\ 20 & 21 & 16 \end{bmatrix}; M * \begin{bmatrix} 9 \\ 19 \\ 20 \end{bmatrix} = \begin{bmatrix} 2 \\ 8 \\ 15 \end{bmatrix}; M * \begin{bmatrix} 24 \\ 21 \\ 2 \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \\ 17 \end{bmatrix}$$

We get numbers 9,19,20,7,4,17 so decrypted word is CIPHER.

Question 3.

(a) Pigpen cipher
Number of possible keys is 26!, Assuming all keys are equally likely $H(k) = log_2(26!) = 88.381953$, for english text $D = 3.2$, and Unicity distance $U = \frac{H(k)}{D} = 27.6194$, that means given at least 28 characters of cryptotext, it should be possible to find unique plaintext and key.

(b) Vigenere cipher
Number of possible keys is 26^n where n is length of key. $U = \frac{H(k)}{D} = \frac{log_2(26^7)}{3.2} = 10.2822$
(11 characters needed)

(c) Transposition cipher with period 7
columns: 1 2 3 4 5 6 7, Transposed columns example: 2 3 4 6 7 1 5
Number of possible permutations is 7!
$U = \frac{H(k)}{D} = \frac{log_2(7!)}{3.2} = 3.8435$ (4 characters needed)

(d) one-time pad
For any alphabetic substitution cipher with a truly random key of length greater or equal to the length of the message, plaintext cannot be found from ciphertext alone. So unicity distance is ∞. Number of possible keys $= \infty$.

Question 4.

(a) K is distributed uniformly: $Pr[K = k_0] = Pr[K = k_1] = Pr[K = k_2] = Pr[K = k_3] = 1/4$

$p_C(0) : Pr[C = 0] =$
$Pr[K = k_0]Pr[P = d_{k0}(0)] + Pr[K = k_1]Pr[P = d_{k1}(0)] +$
$Pr[K = k_2]Pr[P = d_{k2}(0)] + Pr[K = k_3]Pr[P = d_{k3}(0)] =$
$Pr[K = k_0]Pr[P = 3] + Pr[K = k_1]Pr[P = 1] +$
$Pr[K = k_2]Pr[P = 2] + Pr[K = k_3]Pr[P = 3] = \frac{7}{24}$

$p_C(1) : Pr[C = 1] =$
$Pr[K = k_0]Pr[P = d_{k0}(1)] + Pr[K = k_1]Pr[P = d_{k1}(1)] +$
$Pr[K = k_2]Pr[P = d_{k2}(1)] + Pr[K = k_3]Pr[P = d_{k3}(1)] =$
$Pr[K = k_0]Pr[P = 2] + Pr[K = k_1]Pr[P = 0] +$
$Pr[K = k_2]Pr[P = 3] + Pr[K = k_3]Pr[P = 0] = \frac{1}{4}$

$p_C(2) : Pr[C = 2] =$
$Pr[K = k_0]Pr[P = 1] + Pr[K = k_1]Pr[P = 3] +$
$Pr[K = k_2]Pr[P = 0] + Pr[K = k_3]Pr[P = 2] = \frac{1}{4}$

$p_C(3) : Pr[C = 3] =$
$Pr[K = k_0]Pr[P = 0] + Pr[K = k_1]Pr[P = 2] +$
$Pr[K = k_2]Pr[P = 1] + Pr[K = k_3]Pr[P = 1] = \frac{5}{24}$

(b) A cryptosystem has perfect secrecy if $Pr[P = w|C = c] = Pr[P = w]$ or equivalent $Pr[C = c|P = w] = Pr[C = c]$ for all $w \in P$ and $c \in C$.

The specified cryptosystem has not perfect secrecy.

F.e. $Pr[C = 0] \neq Pr[C = 0|P = 0]$ because $(\frac{7}{24} \neq 0)$

$m \backslash e_k$	e_0	e_1	e_2	e_3
0	3	1	2	0
1	2	0	3	1
2	1	3	0	2
3	0	2	1	3

We can change the encryption function e_3 so that the cryptosystem becomes perfectly secure.

Now, for $\forall c \in \{0, 1, 2, 3\}$ hold: $Pr[C = c] = \frac{1}{4}$ and
$Pr[C = c|P = 0] = Pr[C = c|P = 1] = Pr[C = c|P = 2] = Pr[C = c|P = 3] = \frac{1}{4}$

Question 5.

Let $w_i = x_{i,0}\, x_{i,1}\, ...\, x_{i,n}, c_i = y_{i,0}\, y_{i,1}\, ...\, y_{i,n}$. Then we can calculate $w_{i-1} = k_i$ the following way:

$$w_{i-1} = k_i = x_{i-1,0}\, x_{i-1,1}\, ...\, x_{i-1,n} = c_i - w_i = y_{i,0} - x_{i,0}\, y_{i,1} - x_{i,1}\, ...\, y_{i,n} - x_{i,n} \mod 26$$

From this we can calculate w_2 using w_3 and c_3:

$$w_2 = k_3 = c_3 - w_3 = (y_{3,0} - x_{3,0})\, (y_{3,1} - x_{3,1})\, ...\, (y_{3,n} - x_{3,n}) \mod 26$$

Then we can calculate w_1 using w_2 and c_2:

$$\begin{aligned} w_1 = k_2 &= c_2 - w_2 = c_2 - (c_3 - w_3) = \\ &= (y_{2,0} - y_{3,0} + x_{3,0})\, (y_{2,1} - y_{3,1} + x_{3,1})\, ...\, (y_{2,n} - y_{3,n} + x_{3,n}) \mod 26 \end{aligned}$$

And finally we calculate k_1 using w_1 and c_1:

$$\begin{aligned} k_1 &= c_1 - w_1 = c_1 - (c_2 - w_2) = c_1 - (c_2 - (c_3 - w_3)) = \\ &= (y_{1,0} - y_{2,0} + y_{3,0} - x_{3,0})\, (y_{1,1} - y_{2,1} + y_{3,1} - x_{3,1})\, ...\, (y_{1,n} - y_{2,n} + y_{3,n} - x_{3,n}) \mod 26 \end{aligned}$$

4.6 For 26-letter alphabet, determine how many affine ciphers are there that leave

Solution: First of all we have to define the fixed character. From definition of affine cipher for key (a, b) is letter encoded $e_{(a,b)}(w) = a \cdot w + b \mod 26$. Therefore the fixed character is $w \equiv a \cdot w + b \mod 26$, which is equivalent to $-b \equiv (a-1)w \mod 26$. So we have to discus how many solutions have this equivalence. From definiton we know, that $gcd(a, 26) = 1$, therefore $a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$, therefore $(a-1) \in \{0, 2, 4, 6, 8, 10, 14, 16, 18, 20, 22, 24\}$ ($a-1$ is even).

First of all we look at $a = 1$, which is special case: $a = 1 : b \equiv 0 \mod 26$, therefore for $b = 0$ are all characters fixed position and otherwise there are no fixed characters.

For all other a: We know, that $a - 1$ is even and 26 is even too.

- b is odd: This equivalence have no solutions (therefore there are no fixed characters),
- b is even: We can divide both sides of equivalence and modulo too by 2 and we obtain $\frac{b}{2} \equiv \frac{a-1}{2} w \mod 13$. From set of all possible numbers of $a - 1$ we can see that $gcd(a - 1, 13) = 1$, therefore this second equivalence have exactly one solution therefore the original equivalence has exactly two solutions.

We look at all possible values of a and b. □

(a) no characters fixed;

Solution: No fixed characters are for $a = 1$ and $b \neq 0$ and for other possible a and b even. Therefore it is $25 + 11 \cdot 13 = \mathbf{168}$ affine ciphers. □

(b) exactly one character fixed;

Solution: As we can see above all possible options have no fixed or at least 2 fixed characters, therefore there are **0** affine ciphers with one fixed character. □

(c) at least two characters fixed.

Solution: At least two fixed characters are when $a \neq 1$ and b is even and for $a = 1$ and $b = 0$, therefore there are $11 \cdot 13 + 1 = \mathbf{144}$ affine cipher with at least two fixed characters. □

Question 7.

First, determine key length. We do it by overlaying the message with its right rotation and counting letters that are the same, for each rotation 2..20. The results are:

offset	matches
2	58
3	59
4	36
5	80
6	53
7	47
8	42
9	49
10	83
11	44
12	46
13	52
14	45
15	88
16	50
17	48
18	44
19	43
20	74

Clearly the best results are for 15, 10 and 5. As such, it is a good start to assume a key of length 5.

Next, we use frequency analysis on every 5th letter with offset 0..4 to determine the key. We sort the corresponding letters by frequency, creating a frequency list for each position.

Next, we take each frequency list, and for each right shift with offsets 0..25 compute the difference from the English frequency list, which is "ETAOINSRHDLUCMFYWGPBVKXQJZ". We quantify the difference by summing up squares of index differences for each letter. Then we take the lowest difference for each position, giving us:

offset	best shift	best difference
0	16	478
1	6	252
2	23	400
3	12	280
4	8	218

The shift we got is the one needed to "fix" that position. To get the appropriate key, we subtract it from 26, giving us: $10, 20, 3, 14, 18$, or as letters, $KUDOS$.

Deciphered text with this key:

```
WHILEMOSTCRYPTANALYSTSHADGIVENUPALLHOPEOFEVERBREAKINGTHEVIGENE
RECIPHERBABBAGEWASINSPIREDTOATTEMPTADECIPHERMENTBYANEXCHANGEOF
LETTERSWITHJOHNHALLBROCKTHWAITESADENTISTFROMBRISTOLWITHARATHER
INNOCENTVIEWOFCIPHERSINEIGHTEENFIFTYFOURTHWAITESCLAIMEDTOHAVEI
NVENTEDANEWCIPHERWHICHINFACTWASEQUIVALENTTOTHEVIGENERECIPHERHE
WROTETOTHEJOURNALOFTHESOCIETYOFARTSWITHTHEINTENTIONOFPATENTING
HISIDEAAPPARENTLYUNAWARETHATHEWASSEVERALCENTURIESTOOLATEBABBAG
ETOOWROTETOTHESOCIETYPOINTINGOUTTHATTHECYPHERISAVERYOLDONEANDT
    OBEFOUNDINMOSTBOOKSTHWAITESWASUNAPOLOGETICANDCHALLENGEDBABBAGE
    TOBREAKHISCIPHERWHETHERORNOTITWASBREAKABLEWASIRRELEVANTTOWHETH
    ERORNOTITWASNEWBUTBABBAGESCURIOSITYWASSUFFICIENTLYAROUSEDFORHI
    MTOEMBARKONASEARCHFORAWEAKNESSINTHEVIGENERECIPHERCRACKINGADIFF
    ICULTCIPHERISAKINTOCLIMBINGASHEERCLIFFFACETHECRYPTANALYSTISSEE
    KINGANYNOOKORCRANNYTHATCOULDPROVIDETHESLIGHTESTFOOTHOLDINAMONO
    ALPHABETICCIPHERTHECRYPTANALYSTWILLLATCHONTOTHEFREQUENCYOFTHEL
    ETTERSBECAUSETHECOMMONESTLETTERSSUCHASETANDAWILLSTANDOUTNOMATT
    ERHOWTHEYHAVEBEENDISGUISEDINTHEPOLYALPHABETICVIGENERECIPHERTHE
    FREQUENCIESAREMUCHMOREBALANCEDBECAUSETHEKEYWORDISUSEDTOSWITCHB
    ETWEENCIPHERALPHABETSHENCEATFIRSTSIGHTTHEROCKFACESEEMSPERFECTL
    YSMOOTHSIMONSINGHTHECODEBOOK
```

4.8 (a) I finished my second book. It was on the sixth day of Christmas. The manuscript was hidden on the bottom of the seventh drawer of my table. Fortunately, my friend called and said he can come over in three days. At first, I could not believe it. But my four-leg friend Hop greeted John in the door.

Solution: Each sentence contains number n_i. Encryption of this cipher text is the n_i-th letter in the sentence (e. g. in first sentence is number two so the first letter is `f`). The code is `four a. m..` □

(b) ¶↕♣☺‼§↕♣ ○♫ ¶◘♣ ♥☺▬♣

Solution: This symbols are symbol from the beginning of ASCII table and the position of symbol in ASCII table is position of letter in alphabet. The plaintext is `TREASURE IN THE CAVE`. □