Problems of Chapter 1

1.1

1. Letter frequency analysis of the ciphertext:

letter	count	freq [%]	letter	count	freq [%]
A	5	0.77	N	17	2.63
B	68	10.53	O	7	1.08
C	5	0.77	P	30	4.64
D	23	3.56	Q	7	1.08
E	5	0.77	R	84	13.00
F	1	0.15	S	17	2.63
G	1	0.15	T	13	2.01
H	23	3.56	U	24	3.72
I	41	6.35	V	22	3.41
J	48	7.43	W	47	7.28
K	49	7.59	X	20	3.10
L	8	1.24	Y	19	2.94
M	62	9.60	Z	0	0.00

2. ```
Because the practice of the basic movements of kata is the focus and
mastery of self is the essence of Matsubayashi Ryu karate do, I shall
try to elucidate the movements of the kata according to my interpretation
based on forty years of study.

It is not an easy task to explain each movement and its significance,
and some must remain unexplained. To give a complete explanation, one
would have to be qualified and inspired to such an extent that he could
reach the state of enlightened mind capable of recognizing soundless
sound and shapeless shape. I do not deem myself the final authority,
but my experience with kata has left no doubt that the following is
the proper application and interpretation. I offer my theories in the
hope that the essence of Okinawan karate will remain intact.
```
3. Shoshin Nagamine, further reading: *The Essence of Okinawan Karate-Do* by Shoshin Nagamine, Tuttle Publishing, 1998.

### 1.3

One search engine costs \$ 100 including overhead. Thus, 1 million dollars buy us 10,000 engines.

1. key tests per second: $5 \cdot 10^8 \cdot 10^4 = 5 \cdot 10^{12}$ keys/sec
   On average, we have to check ($2^{127}$ keys:
   $(2^{127}\text{keys})/(5 \cdot 10^{12}\text{keys/sec}) = 3.40 \cdot 10^{25}\text{sec} = 1.08 \cdot 10^{18}\text{years}$
   That is about $10^8 = 100{,}000{,}000$ times longer than the age of the universe. Good luck.
2. Let $i$ be the number of Moore iterations needed to bring the search time down to 24h:
   $1.08 \cdot 10^{18}\text{years} \cdot 365/2^i = 1\text{day}$
   $2^i = 1{,}08 \cdot 10^{18} \cdot 365\text{days}/1\text{day}$
   $i = 68.42$
   We round this number up to 69 assuming the number of Moore iterations is discreet. Thus, we have to wait for:
   $1.5 \cdot 69 = 103.5$ years
   Note that it is extremely unlikely that Moore's Law will be valid for such a time period! Thus, a 128 bit key seems impossible to brute-force, even in the foreseeable future.

### 1.5

1. $15 \cdot 29 \bmod 13 \equiv 2 \cdot 3 \bmod 13 \equiv 6 \bmod 13$
2. $2 \cdot 29 \bmod 13 \equiv 2 \cdot 3 \bmod 13 \equiv 6 \bmod 13$
3. $2 \cdot 3 \bmod 13 \equiv 2 \cdot 3 \bmod 13 \equiv 6 \bmod 13$
4. $2 \cdot 3 \bmod 13 \equiv 2 \cdot 3 \bmod 13 \equiv 6 \bmod 13$
```

15, 2 and -11 (and 29 and 3 respectively) are representations of the same equivalence class modulo 13 and can be used "synonymously".

1.7

1.

Multiplication table for Z_4

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

2.

Addition table for Z_5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication table for Z_5

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

3.

Addition table for Z_6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Multiplication table for Z_6

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

4. Elements without a multiplicative inverse in Z_4 are 2 and 0
   Elements without a multiplicative inverse in Z_6 are 2, 3, 4 and 0
   For all nonzero elements of Z_5 exists because 5 is a prime. Hence, all nonzero elements smaller than 5 are relatively prime to 5.

1.9

1. $x = 9 \bmod 13$
2. $x = 7^2 = 49 \equiv 10 \bmod 13$
3. $x = 3^{10} = 9^5 \equiv 81^2 \cdot 9 \equiv 3^2 \cdot 9 \equiv 81 \equiv 3 \bmod 13$
4. $x = 7^{100} = 49^{50} \equiv 10^50 \equiv (-3)^{50} = (3^{10})^5 \equiv 3^5 \equiv 3^2 = 9 \bmod 13$
5. by trial: $7^5 \equiv 11 \bmod 13$

1.11

1. `FIRST THE SENTENCE AND THEN THE EVIDENCE SAID THE QUEEN`
2. Charles Lutwidge Dodgson, better known by his pen name Lewis Carroll

1.13

$$a \equiv (x_1 - x_2)^{-1}(y_1 - y_2) \bmod m$$
$$b \equiv y_1 - a x_1 \bmod m$$

The inverse of $(x_1 - x_2)$ must exist modulo m, i.e., $\gcd((x_1 - x_2), m) = 1$.