MOCK MIDTERM EXAM

1. (a) Define the function φ. **(2 points)**

   (b) Prove that if m, n are positive integers such that $\gcd(m,n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$. **(4 points)**

Solution. (a) The function φ is the counting function of the coprime residue classes, i.e. if $n \in \mathbf{N}$ is given, $\varphi(n)$ is the number of residue classes coprime to n. Formally,

$$\varphi(n) = \sum_{\substack{1 \leqslant d \leqslant n \\ \gcd(d,n)=1}} 1.$$

(b) Assume the prime divisors of m are $p_1, \dots, p_r$, and the prime divisors of n are $q_1, \dots, q_s$. Since $\gcd(m,n) = 1$, we know that these the prime sets are disjoint:

$$\{p_1, \dots, p_r\} \cap \{q_1, \dots, q_s\} = \emptyset.$$

Now the set of prime divisors of mn is the set $\{p_1, \dots, p_r, q_1, \dots, q_s\}$. We learned in the lecture that for any $N \in \mathbf{N}$,

$$\varphi(N) = N \prod_{p:p \text{ is a prime divisor of } N} \left(1 - \frac{1}{p}\right).$$

Applying this formula, we obtain that

$$\varphi(mn) = mn \prod_{i=1}^{r} \left(1 - \frac{1}{p_r}\right) \prod_{j=1}^{s} \left(1 - \frac{1}{q_s}\right) = m \prod_{i=1}^{r} \left(1 - \frac{1}{p_r}\right) n \prod_{j=1}^{s} \left(1 - \frac{1}{q_s}\right) = \varphi(m)\varphi(n),$$

and the proof is complete.

2. (a) Describe the Caesar cipher. **(2 points)**

   (b) Bob encrypts a message using the Caesar cipher and sends it to Alice. Eve intercepts the message, but her time is limited to try only six keys. Independently, Evan also intercepts the message, but his time is also limited, and can try only four keys. What is the probability of that none of them decrypts the message? (Note that Eve and Evan do not consult, it might happen that their attempts overlap.) **(4 points)**

Solution. (a) In the Caesar cipher, both $\mathscr{M}$ and $\mathscr{C}$ are set of the letters of the alphabet:

$$\mathscr{M} = \mathscr{C} = \{\mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d},\mathtt{e},\mathtt{f},\mathtt{g},\mathtt{h},\mathtt{i},\mathtt{j},\mathtt{k},\mathtt{l},\mathtt{m},\mathtt{n},\mathtt{o},\mathtt{p},\mathtt{q},\mathtt{r},\mathtt{s},\mathtt{t},\mathtt{u},\mathtt{v},\mathtt{w},\mathtt{x},\mathtt{y},\mathtt{z}\}.$$

The key set $\mathscr{K}$ is the set of positive integers not exceeding 26:

$$\mathscr{K} = \{k \in \mathbf{N} : 1 \leqslant k \leqslant 26\}.$$

Given a letter, the key k acts on it via a shift by k, where the number corresponding to each letter is its number in the alphabetical order, i.e. `a` is 1, `b` is 2, and so on, `z` is 26. We understand this order cyclically, i.e. after `z`, `a` comes again. To put this more formally,

$$e_k(m) = \text{the shift of } m \text{ by } k \text{ in the alphabetical order, understood cyclically.}$$

As for the decryption, it is a shift backwards by k, or equivalently, a shift by $26-k$. Formally,

$$d_k(c) = e_{26-k}(c).$$

(b) Let us denote by Pr the probability for the scope of this problem. Then

$$\Pr(\text{Eve breaks the cipher}) = \frac{6}{26}, \qquad \Pr(\text{Evan breaks the cipher}) = \frac{4}{26}.$$

Going to the complement events:

$$\Pr(\text{Eve does not break the cipher}) = \frac{20}{26}, \qquad \Pr(\text{Evan does not break the cipher}) = \frac{22}{26}.$$

By assumption, these events are independent, therefore

$$\begin{aligned}
&\Pr(\text{none of Eve and Evan breaks the cipher})\\
&= \Pr(\text{Eve does not break the cipher} \cap \text{Evan does not break the cipher})\\
&= \Pr(\text{Eve does not break the cipher}) \cdot \Pr(\text{Evan does not break the cipher})\\
&= \frac{20}{26} \cdot \frac{22}{26} = \frac{10}{13} \cdot \frac{11}{13} = \frac{110}{169}.
\end{aligned}$$

Therefore, the probability of that none of them breaks the cipher is $110/169$.

3. (a) Describe the XOR cipher. **(2 points)**

   (b) Assume we design a XOR cipher on t bits, where t is even. In order to avoid trivial keys (such as the constant zero key), we restrict to those keys, which contain exactly $t/2$ zeros and $t/2$ ones. Prove that the number of such keys is at least $2^t/t$. **(4 points)**

Solution. (a) In the XOR cipher, we fix a positive integer t, and then

$$\mathscr{M} = \mathscr{C} = \mathscr{K} = \{0-1 \text{ sequences of length } t\}.$$

We define the $\oplus$ operation as the bitwise addition, i.e. if $a = \sum_{j=0}^{t-1} a_j 2^j$, $b = \sum_{j=0}^{t-1} b_j 2^j$ (where a_j, b_j's are binary digits, 0 or 1 each), then let

$$a \oplus b = \sum_{j=0}^{t-1} c_j 2^j,$$

where $c_j = 0$ if $a_j = b_j$, and $c_j = 1$ if $a_j \neq b_j$.

Given m and k, $e_k(m) = m \oplus k$. The decryption function is the same: $d_k = e_k$, i.e. $d_k(c) = c \oplus k$.

(b) The number of those keys which contain exactly $t/2$ zeros and $t/2$ ones is $\binom{t}{t/2}$. Since this is a central binomial coefficient, it is bigger than all the others, i.e.

$$\binom{t}{0} < \binom{t}{1} < \ldots < \binom{t}{\frac{t}{2}-1} < \binom{t}{t/2} > \binom{t}{\frac{t}{2}+1} > \ldots > \binom{t}{t-1} > \binom{t}{t}.$$

Also, $\binom{t}{t/2} \geqslant \binom{t}{0} + \binom{t}{t} = 2$. To sum up,

$$\begin{aligned} \binom{t}{\frac{t}{2}} &\geqslant \binom{t}{0} + \binom{t}{t}, \\ \binom{t}{\frac{t}{2}} &\geqslant \binom{t}{1}, \\ \binom{t}{\frac{t}{2}} &\geqslant \binom{t}{2}, \\ &\cdots \\ \binom{t}{\frac{t}{2}} &\geqslant \binom{t}{t-1}. \end{aligned}$$

The sum of the right-hand sides is 2^t, while the sum of the left-hand sides is $t\binom{t}{t/2}$, i.e.

$$t\binom{t}{\frac{t}{2}} \geqslant 2^t, \qquad \binom{t}{\frac{t}{2}} \geqslant \frac{2^t}{t},$$

and the proof is complete.

4. (a) Describe the discrete logarithm problem in the multiplicative group $\mathbf{F}_p^\times$. **(2 points)**

   (b) Assume that p is an odd prime number, $1 \leqslant g \leqslant p-1$, and a is a positive integer such that $a-g$ is even. Prove that if for some $1 \leqslant x \leqslant p-1$, $g^x \equiv a \bmod p$, then $g^x \equiv a \bmod 2p$. **(4 points)**

Solution. (a) Assume p is a prime number and g is a nonzero residue class modulo p. Assume that for some $1 \leqslant x \leqslant p-1$, $g^x \equiv a \bmod p$, again a residue class modulo p. The discrete logarithm problem is to compute the smallest such positive integer x, if g and a are given.

(b) By assumption $g^x \equiv a \bmod p$. Also, since $x \geqslant 1$, if g and a are both even, then $g^x \equiv 0 \equiv a \bmod 2$, while if g and a are both odd, then $g^x \equiv 1 \equiv a \bmod 2$. In any case,

$$g^x \equiv a \bmod p, \qquad g^x \equiv a \bmod 2.$$

Then $g^x - a$ is divisible by both p and 2. Since p and 2 are coprime numbers, $g^x - a$ is divisible by their product as well, so $g^x \equiv a \bmod 2p$, and the proof is complete.