Final Exam

1. (a) Describe the simple substitution cipher. **(2 points)**

   (b) In Bergengócia (a country in Hungarian fairy tales), people use an alphabet on four characters. How many simple substitution cipher keys k exist for this alphabet which satisfy $e_k = d_k$? **(4 points)**

Solution. (a) In the simple substitution cipher, both $\mathcal{M}$ and $\mathcal{C}$ are set of the letters of the alphabet $\mathfrak{A}$:

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

The key set $\mathcal{K}$ is the group of permutations of $\mathfrak{A}$:

$$\mathcal{K} = \{k : k \in \mathrm{Perm}(\mathfrak{A})\}.$$

Given a letter, the key k acts on it via the permutation, i.e.

$$e_k(m) = k(m).$$

As for the decryption, it is given by the inverse permutation. Formally,

$$d_k(c) = k^{-1}(c).$$

(b) Denote the four characters by w, x, y, z. Any key in question fixes certain letters, and swaps other letters in pairs.

There is exactly 1 key which fixes all the letters. As for those keys which swap one pair of letters and have two fixed letters: the two fixed letters can be chosen 6 ways: $\{w, x\}$, $\{w, y\}$, $\{w, z\}$, $\{x, y\}$, $\{x, z\}$, $\{y, z\}$, and the remaining pair (which is swapped) is determined. Finally, as for the number of keys which swap inside two pairs, there are 3 ways to choose the pair of w, and then the remaining pair is determined. Altogether, there are 10 such keys.

2. (a) Describe the Miller-Rabin primality test. **(2 points)**

   (b) We all know that $15 = 3 \cdot 5$ is not a prime number. Find a *witness*: an integer which is on the one hand coprime to 15, and on the other hand, shows the compositeness of 15 in the Miller-Rabin test. **(4 points)**

   Solution. (a) Let n be a large number (we will assume throughout that it is bigger than 2). If n is even, then it is not a prime. If n is odd, then write $n - 1 = 2^k q$, where $k \in \mathbf{N}$ and q is an odd number (these can be computed in polynomial time). Then pick a certain $1 \leqslant a \leqslant n - 1$, and compute the residue classes $a^q, a^{2q}, a^{2^2 q}, \ldots, a^{2^{k-1} q}$ modulo n, where in this list each residue class is the square of the preceding one (except for the first one, of course), and this list here can be computed in polynomial time. If the list does not start with a 1, and also does not contain a -1, then n is certainly composite: in this case, we say that a is a witness for the compositeness of n.

   The Miller-Rabin test is the following: take many a's, and compute the corresponding list for each of them. If any of the chosen a's is a witness for the compositeness of n, then we reject the primality of n. If none of the chosen a' s is a witness for the compositeness of n, then we accept the primality of n.

   We remark that if n is not a prime, then 75% of the residue classes is a witness for its compositeness. Also, under the Generalized Riemann Hypothesis, there is a witness for the compositeness not bigger than $2 \log^2 n$. The first remark shows that few tests catch compositeness with high probability, i.e. if the number survives few tests, it is safe to say that it is a prime. The second one shows that (conditionally) it suffices to make the test for small a's.

   (b) In case of 15, $k = 1$, $q = 7$. Of course, $a = 1$ will not be a witness, so try $a = 2$ first (it is coprime to 15). Then $2^7 = 128$. This is not ± 1 modulo 15. Therefore, 2 is a witness for the compositeness of 15.

3. (a) Describe the elliptic curve discrete logarithm problem. **(2 points)**

   (b) Let E be the elliptic curve over the field $\mathbf{F}_5$ given by the equation

$$y^2 = x^3 + x + 1$$

   and let $P = (4, 2)$ and $Q = (0, 1)$ be points on E. Compute the point $P + Q$ on E (under the elliptic curve addition). **(4 points)**

Solution. (a) Let E be an elliptic curve. The elliptic curve discrete logarithm problem is, given $P, Q \in E$, to compute the smallest positive integer n satisfying that

$$Q = nP = \underbrace{P + \ldots + P}_{n \text{ times}}$$

holds.

(b) All the computations below are meant in $\mathbf{F}_5$. For the sake of completness, we first record that $P, Q \in E$ (these are straight-forward calculations). Let $y = mx + c$ be the equation of the line passing through P and Q (this is not a vertical line, since $x_P \neq x_Q$). Clearly, $c = 1$ (since $Q \in E$, and $x_Q = 0$, $y_Q = 1$). As for m,

$$m = \frac{y_Q - y_P}{x_Q - x_P} = \frac{-1}{-4} = 4.$$

Now let us substitute $y = 4x + 1$ into the equation of the curve:

$$\begin{aligned} (4x + 1)^2 &= x^3 + x + 1, \\ x^2 + 3x + 1 &= x^3 + x, \\ 0 &= x^3 - x^2 - 2x, \\ 0 &= x(x - x - 2), \\ 0 &= x(x + 1)(x - 2). \end{aligned}$$

Clearly the zeros $x = 0$, $x = -1$ stand for Q, P, respectively. Then for the third intersection point, $x = 2$, and then $y = 4$ from the equation of the line. Then the sum $P + Q$ is $(2, 1)$, after the reflection (or, written projectively, $P + Q = \left[\begin{smallmatrix} 2 \\ 1 \\ 1 \end{smallmatrix}\right]$).

4. (a) Describe the RSA cryptosystem. **(2 points)**

   (b) Prove that the problem of breaking the RSA is polynomially reducible to the discrete logarithm problem in the following sense. Let N be the modulus of an RSA cryptosystem, and assume that there is an algorithm which works as follows: for an input (g, a) satisfying $\gcd(g, N) = \gcd(a, N) = 1$, it computes in polynomial time the output x, where x is the smallest positive integer satisfying $g^x \equiv a \bmod N$ if there is such an x at all, while if there is no such positive integer, $x = \texttt{error}$. Show that using such a hypothetical algorithm, the eavesdropper can decrypt any intercepted cipher in polynomial time. **(4 points)**

Solution. (a) Alice takes two (large) prime numbers p, q, then computes their product N. She also computes $\varphi(N) = (p-1)(q-1)$. Then she takes an exponent $e \in \mathbf{N}$ coprime to $\varphi(N)$, and computes its inverse d modulo $\varphi(N)$. She publishes N, e and keeps $p, q, \varphi(N), d$ in secret.

Now anyone (say, Bob) can send her a message m (a residue class modulo N) using the following protocol. Bob raises the message to power e modulo N and sends $c \equiv m^e \bmod N$ to Alice.

Now Alice raises the incoming cipher c to power d modulo N. With high probability, m is coprime to N, and then, by Euler-Fermat,

$$c^d \equiv (m^e)^d \equiv m^{\varphi(N)u+1} \equiv (m^{\varphi(N)})^e \cdot m \equiv 1 \cdot m \equiv m \bmod N,$$

which is the original message.

(b) Assume Eve intercepts the cipher c. If $c \equiv 0 \bmod N$, then clearly $m \equiv 0 \bmod N$ (since m must be divisible both by p and q). Otherwise, first Eve computes $\gcd(N, c)$. This gcd can be $1, p, q$. If it is p or q, then Eve obtains the factorization of N (since $\{\gcd(N, c), N/\gcd(N, c)\} = \{p, q\}$) and can play the role of Alice from this point on. Assume hence that this gcd is 1. Then $c \in \mathbf{Z}_N^\times$. Now Eve uses her hypothetical algorithm with the input $(c, 1)$. The output t is the smallest positive integer satisfying $c^t \equiv 1 \bmod N$. We claim that $m^t \equiv 1 \bmod N$: indeed,

$$m^t \equiv (c^d)^t \equiv (c^t)^d \equiv 1 \bmod N$$

(whatever d is). Now Eve computes the inverse d' modulo t. Finally, Eve raises c to power d' modulo N:

$$c^{d'} \equiv (m^e)^{d'} \equiv m^{tu'+1} \equiv (m^t)^e \cdot m \equiv 1 \cdot m \equiv m \bmod N,$$

which is the original message.