Final Exam Regulations – read them carefully

1. On the next page, actual Final Exam starts. Please **DO NOT** scroll down until you are ready to take the final.
2. You have a continuous 120 minutes (no breaks) to take the exam. Please, do not make any corrections after this 120-minute window.
3. The final is closed books, no notes, no calculators, no internet. You can use only clean sheets, pens, pencils.
4. You are not allowed to discuss the exam with anyone before the online Farewell Party.
5. Once done, take a scan or a photo of your papers you want to hand in, and send them to me in e-mail. (If possible, send me everything in a single pdf file, where the filename contains your name, e.g. if I took the exam, I would send `magapeter_crypto_final.pdf`. Of course, images in jpg or any other standard file format are accepted.)
6. Please, also sign the statement of honor on this frontpage, and send it to me together with your exam (preferably in the same file).
7. Submission deadline is UTC 6pm, April 22. (I must grade everything by Budapest time 10am, April 23.)

Statement of Honor

I pledge my honor that I do not give or receive any inappropriate aid for this assignment.

signature

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

   (b) Assume $g \in \mathbf{F}_{2027}^\times$. Prove that the smallest positive solution of the discrete logarithm problem $g^x \equiv 1 \bmod 2027$ cannot be 1241. (Note that 2027 is a prime number.) **(4 points)**

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

   (b) Alice and Bob decide to use an XOR cipher on $4t$ bits, where $t \in \mathbf{N}$. They say that a key is "complex enough", if it contains at least t but no more than $3t$ zeros. Prove that more than half of the possible keys is "complex enough". **(4 points)**

3. (a) Describe the elliptic curve Diffie-Hellman key exchange. **(2 points)**

   (b) Over the field $\mathbf{F}_7$, we consider the elliptic curve given by the equation

$$Y^2Z = X^3 + 2XZ^2 - Z^3.$$

   Check that $P = [1, 3, 1]$ and $Q = [2, 2, 1]$ are points of the curve, and compute $P + Q$. **(4 points)**

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

   (b) Alice constructs her own RSA. She chooses the prime numbers $p < q$ in an unfortunate way that $p < \log q$. Prove that Eve can break Alice's system in polynomial time. **(4 points)**