One-Time Pads

Tanya Khovanova

October 5, 2015

Class Discussion

Vigenere Cipher. One-Time Pads. Parity Addition (XORing).

Warm Up

Exercise 1. Two friends went for a walk and found $20. How much money they would have found if there were four of them?

Exercise 2. Parity add 01010100001000011101110 and 10111101010111100010101. Parity add 10111101010111100010101 to the result. What do you notice? Invent a theorem out of this.

Cryptography

Exercise 3. The teachers lounge at AMSA used to be locked with a digital lock with buttons corresponding to five digits: 1, 2, 3, 4, 5. The key was three digits. How many different keys are possible? If the crook Sam punches a digit in half a second, how much time at the most does he need to open the door?

In addition, the lock doesn't have the enter button, which means the crook can save time by overlapping his attempts. If he punches 1, 2, 3 and tries to open the door unsuccessfully, he can then punch 4 and try to open the door again. If the key was 234, the door will open. How much time might he potentially save by this trick?

The crook Michael was smarter and covered the buttons with chocolate ice cream. He came back the next day and noticed that the buttons 2, 3 and 4 were still sticky. He deduced that the key can only have digits 1 and 5.

What is the shortest sequence of punches that Michael needs to guarantee to open the door.

Exercise 4. Decoders sometimes manage to get some extra information. Which piece of knowledge simplifies the decryption of a substitution cipher more: one word known to be "thermometer" or one word known to be "mentor"? Explain.

Exercise 5. The message encrypted with a one-time pad is "ABCDEFGHIJKLMNOKRSTUVW". What is the key, if the messages is "The war starts on Thursday"? What is the key for "Let us have lunch tomorrow"?

Competition Practice

Exercise 6. 1958 Moscow Olympiad. The smallest number of circles of radius 1 that you need to cover the polygon M is a. The largest number of non-overlapping circles of radius 1 with centers inside M is b. What is bigger a or b?

Exercise 7. 1959 Moscow Olympiad. Can you put all three-digit integers that do not end with zero into a sequence such that the last digit of an integer is equal to the first digit of the next one?

Exercise 8. 1959 Moscow Olympiad. A *strobogrammatic* number is a number that looks the same when turned upside down. Let's agree that digits 0, 1 and 8 doesn't change when turned upside down, and digits 6 and 9 switch. The most recent strobogrammatic years were 1881 and 1961. The next strobogrammatic year is 6009. Calculate the number of nine-digit strobogrammatic integers.

Exercise 9. Russian Cryptography Olympiad. Administrator Pete invented the following encoding of digital passwords. The first digit of the password doesn't change, the i-th letter of the encoding ($i > 1$) depends on the $(i-1)$-th and i-th letter of the password. The deciphering can be done uniquely.

The encoded passwords are: 4249188780319, 4245133784397, 5393511, 428540012393, 4262271910365, 4252370031465, 4245133784735. Two passwords corresponding to the list are known: 4208212275831, 4242592823026. Find another password.