

# Classical Cryptography

Tanya Khovanova

September 28, 2015

## Class Discussion

Caesar Cipher. Substitution ciphers. Famous substitution ciphers: Caesar cipher (ROT13), pigpen cipher, Dvorak keyboard, American sign language, Maritime signal flags, ASCII, NATO, Semaphore.

Helpful info:

- Most frequent letters: E — 13%, T — 9%, A — 8%, O — 8%, I — 7%, N — 7%, S — 6%, H — 6%, R — 6%.
- The most common letter at the end/beginning of a word: E/T.
- The most common two/three/four letter words: OF/THE/THAT.
- the most frequent double letters: LL.

Decipher: ZU HO UD CUZ ZU HO ZSGZ AE ZSO JKOEZAUC

## Warm Up

**Exercise 1.** A 100 pounds of cucumbers, that were 99% water, got a bit dehydrated, and became 98% water. What is their weight now?

**Exercise 2.** Which safe lock is better: the one where you need to correctly punch four digits or the one with three letters? Why?

## Cryptography

**Exercise 3.** (due to Martin Gardner) Decipher the answers in the following dialog that were enciphered using the Caesar cipher: What did Mr. MacGregor buy a roll of scotch tape for? svsgl pragf. What did he want it for? gra pragf.

**Exercise 4.** (from cryptograms.org) Decipher the following quotes that was enciphered with a substitution cipher (different cipher for each quote):

Indian prophecy: “CEKN UBMOA MQO KUV M MAOO QUV ROOE PYM XCDE, CEKN UBMOA MQO KUV M AJWOA QUV ROOE SCJVCEOX, CEKN UBMOA MQO KUV M BJVQ QUV ROOE PUYZQM, CEKN MQOE DJKK NCY BJEX MQUM GCEON PUEECM RO OUMOE.”

Madam de Lambert: “NPH GRHVFKWHF XU NPH AXWRY VWH YHZHBNUKR; NPHM GWXCBFH CXWH NPVE NPHM TBIH. NPHM NWXKJRH KF BE FHHQBET NPHC, NPHM YX EXN FVNBFUM KF APHE GXFFHFFBET NPHC VEY NPHM CVQH KF YHFGVBW BE RXFBET NPHC.”

**Exercise 5.** An American spy Nathan was sent to an enemy country. Nathan has a phenomenal memory. So all potentially possible messages to him were numbered and Nathan learned the list by heart. To send him a message the boss sends him an envelope with cash in enemy currency. The total amount is the message. Today Nathan’s boss has an unlimited number of bills but only of 5 and 7 (of whatever denomination the enemy country uses). List all numbers corresponding to messages that can’t be sent.

**Exercise 6.** Michael has a table for a substitution cipher. He is afraid that Tanya can decipher his message. So he decides to apply the cipher twice. Is his message more secure?

## Competition Practice

**Exercise 7. 1949 Moscow Olympiad.** There are 13 coins each weighing an integer number of grams. Any twelve coins can be put into two pans of a balance scale, each containing six coins so that the balance scale balances. Prove that all the coins have the same weight.

**Exercise 8. 1958 Moscow Olympiad.** How many four-digit strings from 0000 to 9999 have the property that the sum of the first two digits equals the sum of the last two digits?

**Exercise 9. 1958 Moscow Olympiad.** Prove that  $n!^2 > n^n$  for  $n > 2$ .

## Optional Homework

Read “The Gold Bug” by Edgar Allan Poe and “The Dancing Men” by Arthur Conan Doyle.