Public Key Encryption

Tanya Khovanova

November 8, 2010

Class Discussion

Public Key Encryption. Digital Signatures.

Warm Up

Exercise 1. A man is trapped in a room. The room has only two possible exits: two doors. Through the first door there is a room constructed from magnifying glass. The blazing hot sun instantly fries anything or anyone that enters. Through the second door there is a fire-breathing dragon. How does the man escape?

Exercise 2. 2004 AMC 8. Three friends have a total of 6 identical pencils, and each one has at least one pencil. In how many ways can this happen?

Exercise 3. 2004 AMC 8. A whole number larger than 2 leaves a remainder of 2 when divided by each of the numbers 3, 4, 5 and 6. Find the smallest such number.

Cryptography

Exercise 4. Prove that for any prime $p \geq 7$ the number $p^4 - 1$ is divisible by 240.

Exercise 5. Russian Cryptography Olympiad. To get to your account at a bank in Wonderland you need to dial a 7-digit password. The bank disconnects the phone as soon as you dial a wrong digit. What is your strategy to get to an account. In how many tries are you guaranteed to brake the password?

Exercise 6. Russian Cryptography Olympiad. Prove that for any prime p the sequence a_1, a_2, a_3, $\ldots$ is periodic with period 2, when a_n is the remainder of p^{n+2} modulo 24.

Exercise 7. Russian Cryptography Olympiad. Is the number $2^{2^{2007}+3^{2008}-2009}-1$ divisible by 1155?

Exercise 8. Russian Cryptography Olympiad. A safe is locked by a round disc with numbers from 0 to 99 written around it in a clockwise direction. The disc is operated by two buttons: left and right. The right button rotates the disc 43 positions clockwise. The left button rotates the disc 20 positions counterclockwise. Currently the marker on the disc points to 0. The safe opens if the marker points to 50. How much time do you need to open the safe if a button click takes one second? Answer the same question for any key (any number instead of 50).

Competition Practice

Exercise 9. 2000 AMC 10. In year N, the 300th day of the year is a Tuesday. In year $N+1$, the 200th day is also a Tuesday. On what day of the week did the 100th day of year $N-1$ occur?

Exercise 10. 2010 MAML. Let S be the set of all five-digit palindromes that are divisible by 11. Find the sum of the digits of the three smallest numbers in S.

Challenge Problems

Exercise 11. Three men are given a challenge. They will all sit in a room and someone will put either a black or a white hat on each one of them with probability one half. The men cannot communicate with each other, but they can see the colors of the hats of the other two men. At the same time, each man says which color they think the hat on his own head is. Each individual can also pass. They win if at least one of them names the color of his hat correctly, and if none of them gives the incorrect answer. How can they maximize their probability of winning?