Cryptography, Combinatorics Intro.

Part 2: Introduction to Combinatorics

The Locked Chest Problem

In medieval times, the inhabitants of a remote village decided to put a number of locks on a giant chest to protect the village valuables from marauding thieves.

For additional security, the villagers created enough locks and keys so that no two people from the village had enough keys to open the chest, but amongst them any group of three people always had enough keys to open all the locks on the chest.

How many locks, and how many keys, are needed to insure that no two people can open the chest, but any three people can?

Food for thought…

Let's think about this problem as a group. A good way to solve a big problem is to ask lots of questions. What are some good questions that we could consider about this situation?

What are some useful assumptions or facts about the situation?

Try a simple, specific situation.

What if there are 3 people in the village? How many keys and locks are needed?

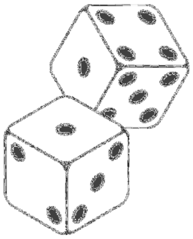
What if there are 4 people in the village? How many keys and locks are needed?

A Brief Introduction to Combinatorics

Combinatorics is the branch of mathematics that studies methods of counting elements in a set, their orderings, and possible combinations. The field of combinatorics intersects cryptography when we need to count the number of possible combinations or arrangements of some numbers to make sure that an encrypted message is secure.

Counting Order

Counting is a central topic in combinatorics. The **counting principle** is something that you have probably run into when studying probability.



Problem 1: How many outcomes are possible when three dice are rolled together, if no two of them are the same?

Problem 2: Suppose you have a 5 letter (with unique letters) word in which we have scrambled the letters in a cryptographic attempt to disguise the original message. How many possible orders can there be when you rearrange the 5 (unique) letters?

(Extra challenge: what if 2 of the letters are the same? Or 3 of the letters?)

Definition: The expression $n!$ is read "n-factorial" and represents

$$n! = n(n-1)(n-2)(n-3)\cdots 1$$

Let's revisit the Lock problem…

Problem 3: Suppose there are 10 keys numbered 1 through 10, and you have to choose 3 of them and place them *in a line*. How many different outcomes are there?

Definition: The number of *permutations* of n items taken k at a time is

$$P(n,k) = {}_nP_k = n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}$$

Making Choices

Now, what sometimes we want to choose objects, but we don't care about the order.

Problem 4: Now, suppose there are 5 different types of keys in your village numbered 1 through 5. You decide that you are going to give each villager 2 keys, but we don't care about the order they are in? (So, the combination of keys 3&4 is the same combination as having keys 4&3).

<u>**Definition:**</u> The number of *Combinations* is the number of ways to choose of k <u>unordered</u> items from n possibilities. This is also known as the *binomial coefficient* and read "n choose k":

$$C(n,k) =_n C_k = \binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

Problem 5: If there are 10 people in the village and two people are going to approach the locked chest, how many different combinations of 2 people can approach the treasure chest?

In how many ways can 3 people approach the treasure chest?

Problem 6: Suppose that there are 6 locks (numbered L1, L2, ..., L6) on the chest. If each person is given a keyring with 4 keys (each to different locks), how many *different* combinations of keyrings could be made.

What does this imply for our village?

Finding the Treasure in the Math

Now that we have the tool of Combinations to define the "number of ways to choose", Let's try rephrasing some of the important questions relating to our original problem.