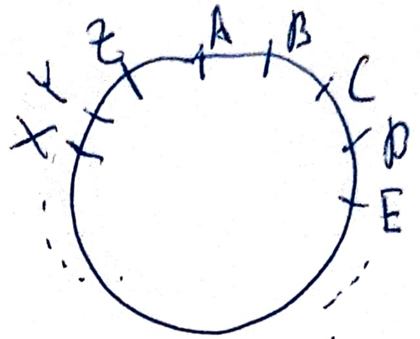
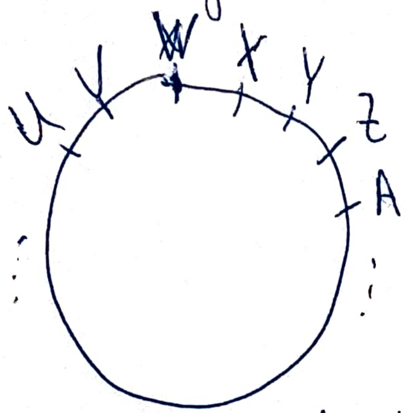
Simple substitution ciphers

In order to produce such an encoding, 'put the letters, equidistant on a wheel', i.e.



and rotate it, say, clockwise by $0 \leq k < 26$ units:



Substitute each letter by the one on the same position after the rotation. In our example

$A \to W$
$B \to X$
$C \to Y$
$\vdots$

<u>Def-n</u>: such a cipher is called a <u>shift cipher</u> or <u>Caesar cipher</u>. The original message is referred to as the <u>plaintext</u> and the one obtained via the substitution the <u>ciphertext</u>.

Example. Plaintext: HELLO Shift by $k=5$.
$\downarrow\downarrow\downarrow\downarrow\downarrow$
Ciphertext: CZGGJ

Rmk: how many shift ciphers are there? Answer: 26 (one of which is trivial). Very fast to decrypt!

More general version: simple substitution ciphers (each letter is replaced by another letter). We impose the requirement that different letters are substituted by different ones. In other words the map

$$\{a,b,c,\dots,z\} \longrightarrow \{a,b,c,\dots,z\} \text{ is a bijection.}$$

Question: how many such maps are there?

Answer: 26!

What is an example of a simple substitution cipher which is not a shift?

$A \leftrightarrow Z$, the other letters are fixed.

$(26!-26)$ such ciphers exist!

Is it easy to break a simple substitution cipher?

Answer: it is. The reason is that the letters in plaintext have patterns. Namely, some letters appear much more often than the others, frequently words end with 'ing' or 'ty', etc.

Alternative description of simple substitution ciphers.

Let us encode the letters by numbers via

$A \leftrightarrow 1$

$B \leftrightarrow 2$

$\vdots$

$Z \leftrightarrow 26.$ (SSC)

A simple substitution cipher is a map

$f: \{1,2,\dots,26\} \to \{1,2,\dots,26\}$, such that

(*) $f(i) \neq f(j)$ if $i \neq j$

Such maps are called permutations and there is a group structure on them. Thus obtained group is called symmetric. Symmetric groups are the most important finite groups (the underlying set has finitely many elements) and we will discuss them in more detail later.

Def-n. A map f is said to fix an element i if $f(i)=i$.

Questions:

(1) How many SSC fix 25 elements?

(2) How many SSC fix 24 elements?

(3) How many SSC fix 23 elements?

Answers:

(1) If f fixes 25 elements (say, all elements (possibly) except some element i), than $f(j)=j$ for any $j \neq i$. Since $f(i) \neq f(j)$ for $i \neq j$, the only possibility is $f(i)=i$. In other words $f(j)=j$ for all j and there is only one such map. It is called <u>identity</u> (and corresponds to the unit element in the group).

(2) First we choose the 24 elements that are fixed and there are $\binom{26}{24}=\binom{26}{2}$ such choices. The remaining 2 elements can not be fixed, hence, must be swapped (i.e. if these elements were i and j, then $f(i)=j$ and $f(j)=i$, the corresponding group element is called <u>trans-position</u>). Therefore, there are $\binom{26}{24}$ such maps.

(3) Similarly, we choose the 23 fixed elements (say, all except i, j and k, for a particular map). Then we must have $f(i) \neq i$, $f(j) \neq j$, $f(k) \neq k$. Also, as 'all the other places are occupied', $f(i) \in \{j,k\}$, $f(j) \in \{i,k\}$, $f(k) \in \{i,j\}$ and $f(i), f(j), f(k)$ are pairwise distinct. There are only two possibilities:

$$\begin{matrix} i \to j \\ j \to k \\ k \to i \end{matrix} \quad \text{or} \quad \begin{matrix} i \to k \\ j \to i \\ k \to j \end{matrix}$$

, giving the answer $\binom{26}{23} \cdot 2$.

What if we choose an arbitrary number k between 0 and 25 and ask how many permutations fix exactly k elements?

Well, again we choose the k fixed elements (in $\binom{26}{k}$ ways) and for each such choice none of the remaining elements can be fixed. Let D_k be the number of permutations of k elements with no fixed elements (such permutations are called <u>derangements</u>). Then the answer is given by

$$\binom{26}{k} \cdot D_k .$$

So it remains to find D_k (we already know that $D_2 = 1$ and $D_3 = 2$).

If you are interested in finding this numbers and (or) would like to get a few extra-credit points, take a look at the 'Bonus 1' set of problems.

Divisibility and GCD.

The main goal of Cryptography is to create a cipher that is very hard (ideally impossible) to decode. The search for such ciphers naturally leads to working with numbers (as we first encode every letter with a number and the computers understand everything in numbers, bits to be precise). Therefore, we will spend a lot of time learning the properties of numbers. The corresponding area of mathematics is called Number Theory.

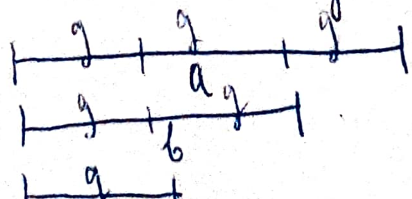
Def-n. Let a, b be two positive integers. Then GCD(a,b) is the largest integer that divides both a and b. It is called the greatest common divisor of a and b.

Examples:

(0) GCD$(3,5)=1$ (1) GCD$(2,8)=2$ (2) GCD$(16,8)=8$.

How can we efficiently find the GCD?

The following algorithm appears in Euclid's Elements (c.300 BC). It was formulated in a more geometric way. The GCD of two lengths a and b is the greatest length g that measures a and b evenly, i.e. a and b are integer multiples of g:



Algorithm (we use the values $a=242$, $b=54$)

	Geometrically	Algebraically
Step 1.	54 | 54 | 54 | 54 | 26 | 242	$242 = 54\cdot 4 + 26$
Step 2.	26 | 26 | 2 | 54	$54 = 26\cdot 2 + 2$
Step 3.	$\underbrace{2\,\vert\,2\,\vert\,2\,\vert\,2\,\vert\,2\,\vert\,2\,\vert\,2\,\vert\,2\,\vert\,2\,\vert\,2\,\vert\,2\,\vert\,2\,\vert\,2}_{13 \text{ intervals}}$ 26	$26 = 2\cdot 13 + 0.$
Step 4	2	$GCD(242,54)=2$

We demonstrate the algorithm on one more example.

$GCD(210,45)=?$

$210 = 45\cdot 4 + 30$

$45 = 30\cdot 1 + 15$

$30 = 15\cdot 2 + 0$

$GCD(210,45)=15$

Remark 1: $GCD(a,b)$ is the first number that fully divides the preceding one in the sequence $\{a, b, r_1, r_2, \dots\}$, where r_1 is the remainder of a/b, r_2 is the remainder of b/r_1, etc. In the example above $a=210$, $b=45$, $r_1=30$, $r_2=15$. and 15 divides 30.

Remark 2. GCD(a,b) divides both a and b, hence divides their residue $r_1 = a - k_1 b$ as well $(0 \leq r_1 < b)$. Similarly, we establish that GCD(a,b) divides r_2, r_3, etc. Since the sequence $\{a, b, r_1, r_2, \ldots\}$ is strictly decreasing and consists of positive integers, the algorithm converges after finitely many steps.

Extended Euclid's algorithm.

Our next goal is to establish the following result.

Thm 1. Let $x, y \in \mathbb{Z}_{>0}$ and $c = GCD(x,y)$. Then $\exists a, b \in \mathbb{Z}$, such that $ax + by = c$.

The proof is constructive (actually allows to find a and b, rather than just shows their existence). We will demonstrate it on a concrete example. The general argument is completely analogous.

$x = 1398, \quad y = 324$

$1398 = 4 \cdot 324 + 102$

$324 = 3 \cdot 102 + 18$

$102 = 5 \cdot 18 + 12$

$18 = 12 + 6$

$12 = 2 \cdot 6 + 0$

$c = GCD(1398, 324) = 6$

$6 = 18 - 12 = 18 - (102 - 5 \cdot 18) =$

$= 6 \cdot 18 - 102 = 6 \cdot (324 - 3 \cdot 102) -$

$- 102 = 6 \cdot 324 - 19 \cdot 102 =$

$= 6 \cdot 324 - 19 \cdot (1398 - 4 \cdot 324) =$

$= 82 \cdot 324 - 19 \cdot 1398$, so

$-19 \cdot 1398 + 82 \cdot 324 = 6$

$a = -19$ and $b = 82$.