Cryptography Worksheet — Mono-alphabetic Substitution 1

In the Atbash and Pigpen Ciphers we replaced each letter with the same letter or symbol each time. In the Caesar Cipher, we shifted the alphabet, but kept it in the same order. For the Affine Cipher, we followed a specific rule to work out what we should replace each letter by.

What do all these ciphers have in common?

We call this type of cipher a **Mono-alphabetic Substitution Cipher**. *What do you think this means?*

There is an even more general version of this type of cipher. When we looked at the Caesar Shift, remember that the alphabet was shifted, but remained in the same order (and it returned to the beginning when it reached “Z”). However, we do not have to keep the alphabet in the same order. Below is an example of a ciphertext alphabet that is in a random order.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
H	N	X	E	L	B	T	J	D	Z	K	R	Q	C	M	A	W	Y	G	S	V	I	O	F	P	U

Using the table, decipher the message:

ZHCVH YPNYD CTGSJ LGCMO

Using the same table, write a short message to a friend, and get them to decipher it.

In using this cipher, what is the key?

The Martian Alphabet only has 3 letters - 🟥 , ▲ and 🟢

How many different ways are there of ordering the ciphertext alphabet for the Martian Alphabet?

The Venusian Alphabet has the same symbols as the Martians, along with the extra symbol ⬟

How many different keys are there for the Mono-alphabetic Substitution Cipher on the Venusian Alphabet?

How many keys would there be for an alphabet containing 5 letters?

Can you deduce how to work out how many keys there will be for an alphabet of length n?

How many possible keys are there for our alphabet of 26 letters.

Cryptography Worksheet — Mono-alphabetic Substitution 2

We have seen that there are many different keys for the Mono-alphabetic Substitution Cipher. In order to use the cipher, the sender and receiver must agree on one of these keys before enciphering any messages, so that they know what ciphertext alphabet to use when enciphering or deciphering the message.

How could you come up with an easy to remember way of generating the ciphertext alphabet?

The most commonly used method, is to use a *keyword*, which generates the key. Usually this is implemented as follows. The keyword is chosen as a memorable word to both the sender and the receiver. To generate the key (the ciphertext alphabet), you first use the letters from the keyword in the order they appear in the keyword (but without repeating any letters). Once all the letters from the keyword have been used, you now insert the remaining letters of the alphabet in alphabetical order.

Why do you not repeat letters that appear in the Keyword more than once?

Using the Keyword “MATHEMATICS”*, complete the table below showing the ciphertext alphabet.*

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
M	A	T	H																						

Are there any weaknesses with the ciphertext generated by this keyword? What has caused these?

How could you overcome these weaknesses when choosing a keyword?

Using the keyword “ZEBRAS”*, encode the plaintext*:

“Such stuff as dreams are made of”.

Again using the keyword “ZEBRAS”*, decode the following message*:

“KLQDFKC BZK BLJA LS KLQDFKC”.

With your partner decide on a suitable keyword. Individually, generate the ciphertext alphabet from your keyword, and encode a short message using it. Swap messages, and decode.

Teacher's Notes — Mono-alphabetic Substitution

Worksheet 1

The Atbash, Pigpen, Caesar Shift and Affine Ciphers are all examples of Mono-alphabetic Substitution ciphers. That is, they are substitution ciphers (so each letter is replaced with something), and they are mono-alphabetic because each letter is always replaced by the same letter or symbol.

Discuss that you do not need to have the alphabet in order, or in an order generated by the Affine Cipher. There are actually many more ways that you can order the alphabet, but the important thing is that each letter of the plaintext alphabet is enciphered to one letter of the ciphertext alphabet, and that no two letters are enciphered to the same letter (i.e. it must be a one-to-one mapping). Remind them when deciphering the message, that it is given in blocks of 5 as a convention, and that the spaces are not necessarily spaces in the plaintext.

The message is: "January brings the snow".

The key for the example cipher given is the order of the alphabet.

For the Martian Alphabet, there are 6 different substitution ciphers possible. Explain that this means, for the Martian Alphabet, there are 6 different keys for the general Mono-alphabetic Substitution Cipher.

For the Venusian Alphabet, there are 24 different keys that can be used. Note that one of these is the identity key, which does nothing to the letters. For an alphabet of 5 letters, there are 120 different keys.

In general, for an alphabet of n letters there are $n!$ keys, where

$$n! = n \times (n - 1) \times (n - 2) \times \ldots \times 3 \times 2 \times 1$$

For our English Alphabet of 26 letters, there are 26! possible keys. That is

403, 291, 461, 126, 605, 635, 584, 000, 000

Which is just over 400 million million million million. That is a huge number, and if every single person on earth (say 6 billion) tried one key a second, it would take 2,137,236,834 years to test every single key to break a code!!!

Discuss how it is hard for an individual to remember a list of 26 letters in order (ask them to think about how long it takes to learn the alphabet).

Teacher’s Notes — Mono-alphabetic Substitution

Worksheet 2

There are many different keys for the Mono-alphabetic Substitution Cipher, and in order to use the cipher, the sender and receiver must agree on one of these keys before enciphering any messages.

Discuss how it is hard for an individual to remember a list of 26 letters in order (ask them to think about how long it takes to learn the alphabet). Off of this discussion, ask them to think (maybe in small groups or pairs) of ways that they could generate the ciphertext alphabet, which would be easy to remember for both parties.

The method that is usually used in real life is using a keyword. Given a keyword, the letters from the keyword are the first letters used in the ciphertext alphabet (ignoring any repeated letters), and these are followed by the rest of the letters of the alphabet that have not already appeared in alphabetical order. For example, if the keyword is “MATHEMATICS”, then we would get the ciphertext alphabet shown below, since we write the letters of the keyword first “MATHE”, but then we do not write the “M” again. We do this for all letters in the keyword, and then we start the rest of the alphabet with “B” (as we already have “A”).

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
M	A	T	H	E	I	C	S	B	D	F	G	J	K	L	N	O	P	Q	R	U	V	W	X	Y	Z

The reason you do not repeat letters in the ciphertext alphabet is that you need a one-to-one mapping between plaintext and ciphertext. That is, if you used the same letter more than once, then more than one plaintext letter would be enciphered as that ciphertext letter, which would make the message impossible to decipher.

One weakness of this keyword is the fact that many letters are replaced by themselves : “e”, “u”, “v”, “w”, “x”, “y” and “z”. In this case, “e” is a coincidence, but the last 6 letters of the alphabet map to themselves for a reason. All the letters afters the last alphabetical letter within the keyword will map to themselves. In this case, “T” is the last letter alphabetically in the word “MATHEMATICS”, and all the letters after “T” in the alphabet map to themselves. For this reason it is usually a good idea to choose a word with at least one of the letters from towards the end of the alphabet.

The keyword “ZEBRAS” generates the ciphertext alphabet below, and the encoded message should read “PTBD PQTSS ZP ROAZJP ZOA JZRA LS”.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Z	E	B	R	A	S	C	D	F	G	H	I	J	K	L	M	N	O	P	Q	T	U	V	W	X	Y

The message decodes as “Nothing can come of nothing”.