Ciphers

Caesar's Shift

Lecture notes of Alexander Wood
CSCI 360 Cryptography and Cryptanalysis
awood@jjay.cuny.edu

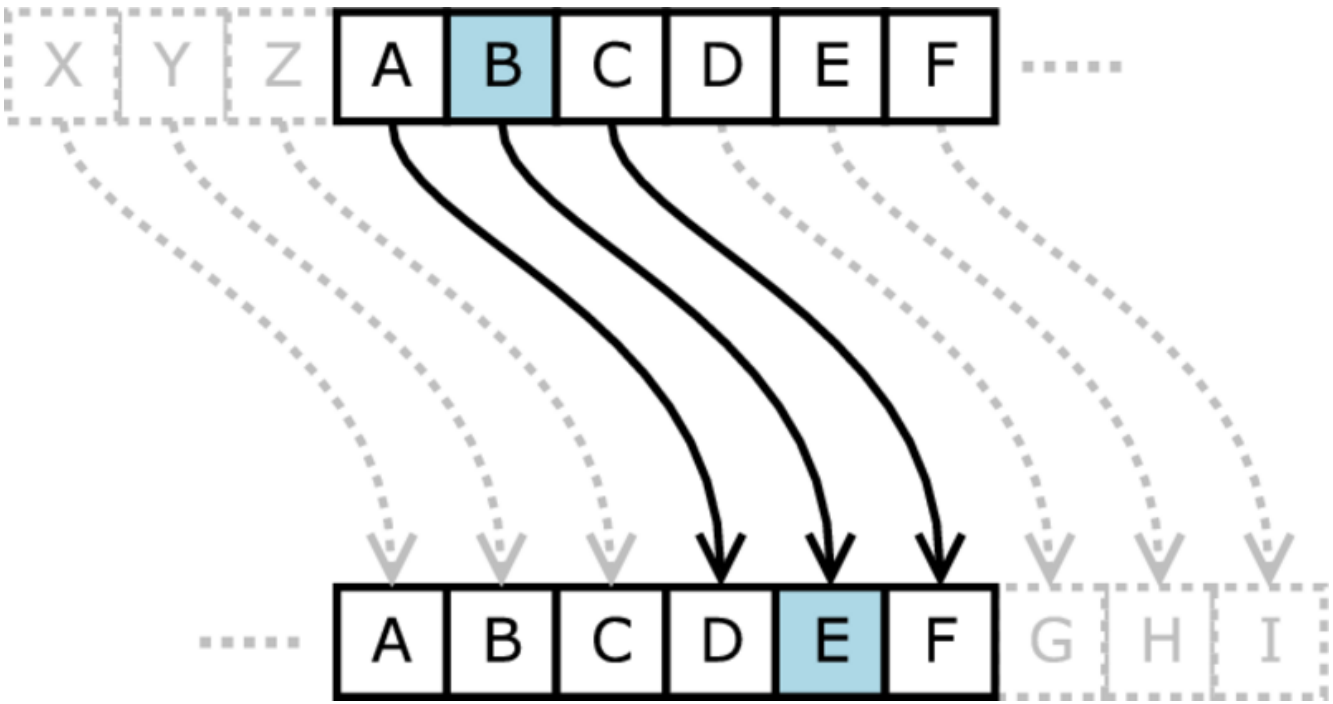
John Jay College of Criminal Justice

Caesar's Shift

The first cryptosystem we will look at is called **Caesar's Shift**. This cipher is one of the earliest ever invented – it was used by Julius Caesar to disguise communication!

The Original Cipher

In Caesar's original cipher, every letter was shifted exactly three letters to the right. Note that X, Y, and Z are brought around to the beginning and shifted to A, B, and C, respectively.



The Original Cipher

This is perhaps better visualized as a circle! In this photo, the plaintext is on the outside, and the ciphertext is on the inside. To encrypt a phrase, match each letter on the outside to a letter on the inside. To decrypt, match each letter on the inside to the corresponding letter on the outside.

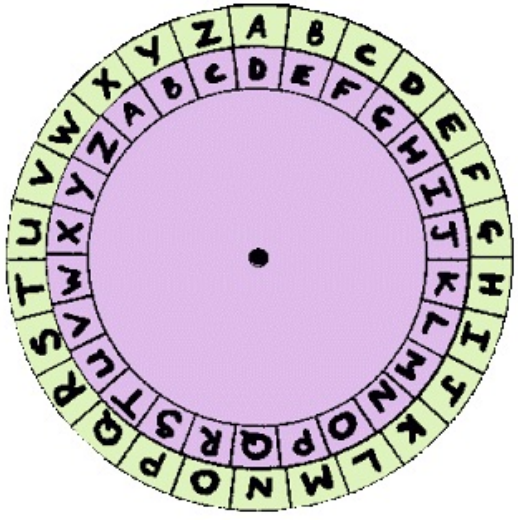
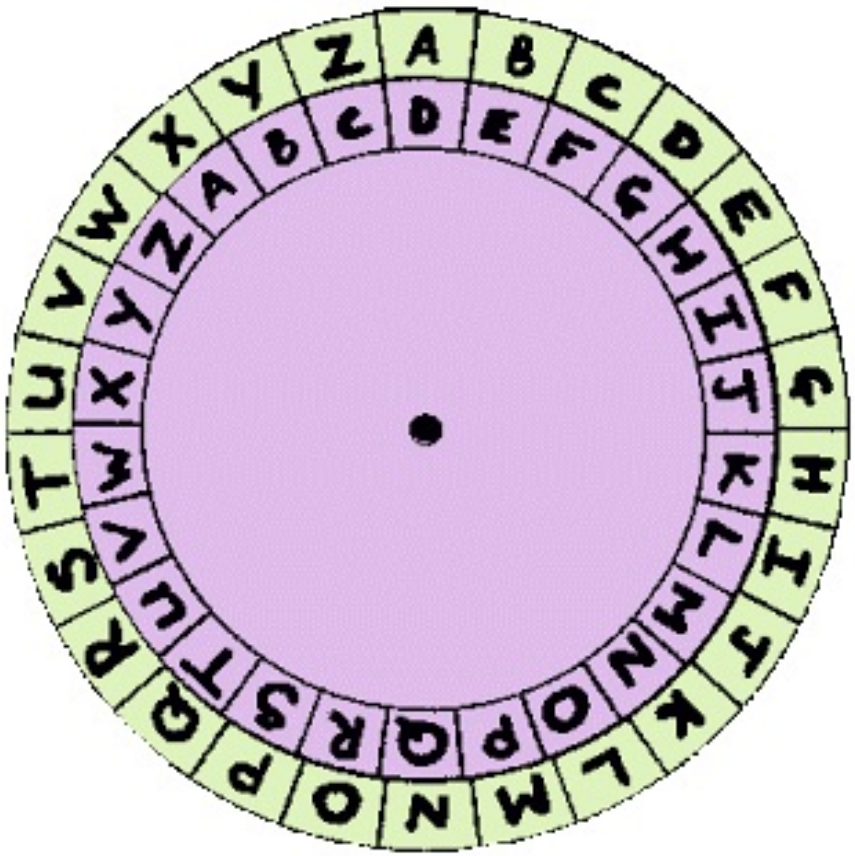


Image from
`http://dubworks.blogspot.com/2013/10/some-exercises-with-caesar-cipher-with_22.html`

Exercise 1

Use the wheel below to decrypt the message:

KRWOLQH EOLQJ



Shift Ciphers

Of course, we can also shift the alphabet differently! Instead of shifting three letters, we could shift seven, or twenty, or fifteen!

I Got The Keys

Let's call Caesar's original cipher a **3-shift**, because we shifted each letter three to the right.

keys, keys, keys

How many different possible shifts are there?

Keys and Keyspaces

The **keyspace** of the shift cipher is 25, and the key is a number in the range 1 through 25.

Exercise 2

Say the key is $K = 19$, with a shift corresponding to the wheel below.

What is the decryption of IHDXFHG?

Exercise 3

Use a Caesar's Cipher Encypter at

`https://lingojam.com/CaesarCipher`

Go ahead and encrypt any message you want!

Exercise 4

Use the Caesar's Cipher Decrypter at

`http://www.mygeocachingprofile.com/codebreaker.caesarcipher.aspx`

To decrypt the following phrases and keys:

(a) TSOIFEPP KS, $K = 4$

(b) PK XA KN JKP PK XA PDWP EO PDA MQAOPEKJ, $K = 22$

(c) JYV JVCCJ JVRJYVCCJ SP KYV JVRJYFIV, key unknown!

Coding Exercise 1: Caesar's 3-Cipher

First, let's use Python to encrypt using Caesar's original cipher, which shifts every input three letters to the right. Let's write a function called `encrypt` which encrypts using Caeser's 3-cipher, as well as a corresponding `decrypt` function.

Coding Exercise 1: Caesar's 3-Cipher

Write Python code for the following functions using Caesar's 3-shift.

```
encrypt
INPUT: plaintext string
OUTPUT: ciphertext string

decrypt
INPUT: ciphertext string
OUTPUT: plaintext string
```

Coding Exercise 2: Shift Cipher

Now let's code the shift cipher with *any* key. Our functions `encrypt` and `decrypt` must now take on a second argument, `key`.

Coding Exercise 2: Shift Cipher

Write Python code for the following functions using the shift cipher.

```
encrypt
INPUT: plaintext, key
OUTPUT: ciphertext

decrypt
INPUT: ciphertext, key
OUTPUT: plaintext
```

References

- Caesar's Shift Encrypter:
  `https://lingojam.com/CaesarCipher`
- Caesar's Shift Decrypter:
  `http://www.mygeocachingprofile.com/codebreaker.caesarcipher.aspx`
- The Assigned Reading: Schneier's *Applied Cryptography* pages 10-13
- Our other textbook *Invent With Python* has a chapter on Caesar's cipher with another Python implementation:
  `http://inventwithpython.com/hacking/chapter6.html`
- C++ and Java implementations:
  `http://www.geeksforgeeks.org/caesar-cipher/`