It's All Code

Minnesota State Community and Technical College

Moorhead

Reason

- Why do people need to send secret messages?
- How can messages be coded?

Bob and Alice want to send messages to each other, in secret. We don't know why they want to communicate. How can Alice and Bob secretly communicate over the Internet?

Very Simple Code

- Open Word
- Type a secret message
- Do not let the people next to you see the message
- Change the font to Wingdings or Symbol
- Move one seat to the left
- Decode the message
- Easy?

This is very easy, but not very secure. Julius Caesar had a similar problem. We will try his solution.

Caesar

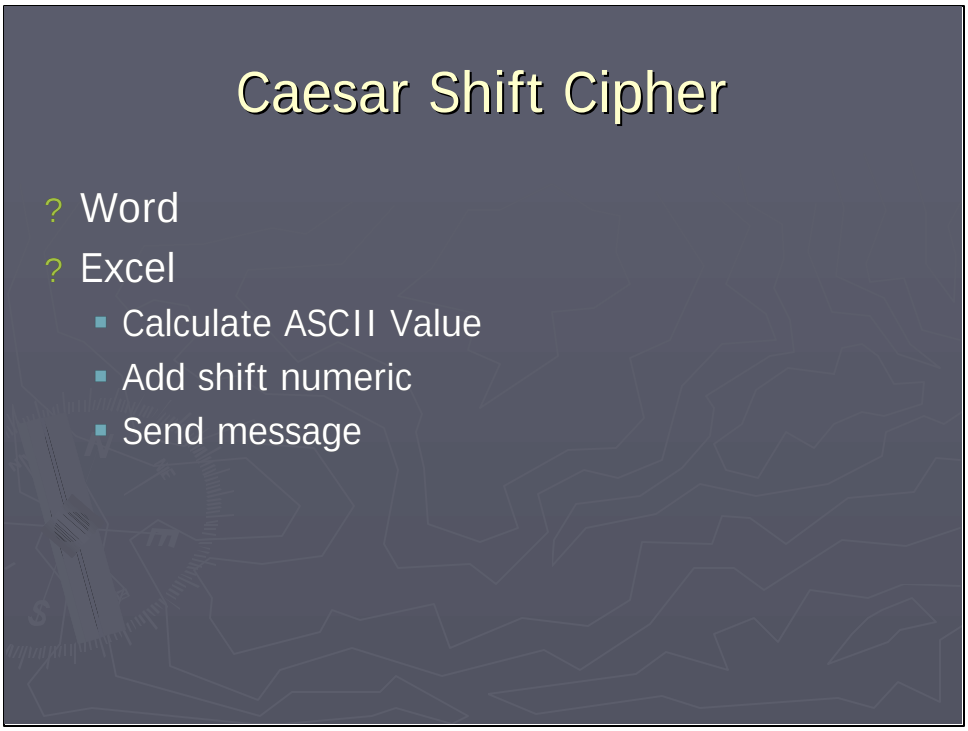
- Julius Caesar encryption situation
  - Secret military messages to send
  - 50 AD
  - ENIAC 1947
  - ASCII 1968 standard
  - What to do?
- Answer
  - Caesar Shift Cipher

"It is this idea of symbol substitution that we are interested in when we consider the concept of Caesar Shift Cipher. Around 50 BC, Julius Caesar developed the idea of transposing letters in the alphabet in order to transmit military messages with relative security. In this code, each letter is replaced by a letter three places down in the alphabet (i.e. the letter 'a' is replaced with the letter 'd' or the letter 'b' is replaced with the letter 'e'). Although this code may seem rather simplistic today, it more than met security desires in an age where illiteracy was widespread."

http://cse.unl.edu/~bholley/Cypher%20Tutorial.html

Julius Caesar had secret military messages to send. Unfortunately, the messages needed to be delivered about 50 BC, a couple of year before ASCII code and the modern computer.

Caesar Shift Cipher works by substituting each letter in the message with a letter three letters down the alphabet. The substitution would wrap around the alphabet.



One way to use the Caesar Shift Cipher is write the message in Word. Then manually convert each letter to the same character three character away.

Another way to use the Caesar Shift Cipher is to use Excel to do the work. Excel can convert each character to ASCII numeric. As a spreadsheet, Excel can add three or whatever number to the ASCII value and give us a new character.

Excel Notes

- =CODE(A1) give ASCII code give ASCII character for cell A1 character
- =CHAR(A2) gives ASCII character for cell A2 number
- You may not generate a number greater than 255

In Excel, functions are identified by an equal sign in front. The function keyword is second. Finally, in parenthesis is the cell letter/number.

Code a document

- Put each letter of your secret message in a single Excel cell
- Input the function to generate ASCII code, =CODE()
- Add the required number to the code
- Generate the new cipher, =CHAR()
- Copy the cipher into Word
- Destroy the spreadsheet

The easiest way is create the message in Excel. Give each letter it's own cell. Excel can't handle more than one character per cell.

Example:

After the cell number is an example of what is in the cell.

A1,	A
A2,	=CODE(A1)
A3,	=A2+3 [does the three letter shift]
A4,	=CHAR(A3)

The secret letter is in A4

Copy and paste the message in Word and destroy the spreadsheet

Decode a document

- Move five chairs to the right
- Decode the message

This may take some time.

Encryption Problems

- Caesar Shift Cipher uses private key encryption
- How to safely exchange private keys
- Diffie-Hellman solution is public – private key encryption
- RFC 2631 describes Diffie - Hellman

This is optional.

References

- http://jfg.girlscouts.org/GS/insignia/Badges/tech/computerfun.htm
- http://www.trincoll.edu/depts/cpsc/cryptography/caesar.html
- http://cse.unl.edu/~bholley/Cypher%20Tutorial.html
- http://www.jimprice.com/jim-asc.htm
- http://www.ietf.org/rfc/rfc2631.txt