

# ***Cryptography***

- By Mecedez Griner, Steve Quella,  
and Ben Geels

# ***What is cryptography?***

- cryp·tog·ra·phy n.
  - The art and science of keeping information secure from unintended audiences, by encrypting it.
  - Secret writing.
  - The Process or skill of communicating in or deciphering secret writings or ciphers.
- Essentially cryptography is about a code, or method of translating, so to speak, from one language into another.
  - It can take many forms; even foreign language is a sort of code to those who can only speak English.

# *Key Terms*

- Cipher – an algorithm for performing encryption
- Decipher or Decryption – To decode the encrypted message.
- Key – the parameter (piece of information) which controls the algorithm for encryption.

# *History*

- Cryptography is one of the oldest fields of technical study we can find records of, going back at least 4,000 years.
- Cryptography probably began in or around 2000 B.C. in Egypt, where hieroglyphics were used to decorate tombs of deceased rulers and kings.
- Cryptography was, and still is, used in army/navy settings where the officers are trying to encode operations from the enemy intelligence.

# *Caesar Cipher*

- The method is named after Julius Caesar, who used it to communicate with his generals.
- The encryption of a text phrase by shifting the position of the letters by a certain value.
- The letters of the alphabet can be represented by numbers with a equaling 0, b equaling 1 and so on, and with the certain shift value can be added to the letters in the text to receive the encrypted message.

# *Operation*

- Start with the first letter of the text you want to decipher.
- Add the key to it.
- Divide by mod  $m$ .
  - $M$  being the range of your text
  - In our alphabet the range would be 26
- Then move on to the next letter and repeat.

# ***Decryption***

- Almost identical process.
- Start with the first letter of the text you want to decipher.
- Subtract the key from it.
- Divide by mod  $m$ .
- Then move on to the next letter and repeat.

# *Hill Cipher*

- Invented by Lester S. Hill in 1929
- It was the first polygraphic substitution cipher in which it was practical (though barely) to operate on more than three symbols at once.

# *Operation*

- Each letter is first encoded as a number.
  - i.e.  $A = 0, B = 1, \dots, Z = 25$
- A block of  $n$  letters is then considered as a vector of  $n$  dimensions, and multiplied by an  $n \times n$  matrix, modulo 26.
  - The  $n \times n$  matrix must be invertible (has a determinant not equal to zero) and the determinant must not have any common factors with 26

# ***Decryption***

- We turn the ciphertext back into a vector,
- Then simply multiply by the inverse matrix of the key matrix.

# ***Playfair cipher***

- Also known as a Playfair square - it is a manual symmetric encryption technique and was the first literal cipher.
- The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher.

# Operation

- The Playfair cipher uses a 5 by 5 table containing a key word or phrase.
- To create the table you must...
  - fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters)
  - then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "X" to reduce the alphabet to fit, other versions put both "I" and "J" in the same space)
  - The keyword can be written in the top rows of the table. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key.
- To encrypt a message break the message into digraphs (groups of 2 letters) then follow these four rules...
  - If both letters are the same (or only one letter is left), add an "X" after the first letter.
  - If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
  - If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).

If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

# ***Decryption***

- To decrypt, use the INVERSE (opposite) of the first 3 rules, and the 4th as-is (dropping any extra "X"s (or "Q"s) that don't make sense in the final message when finished).
- Replace any i's with j's that fit and vice versa.

# *Vigenere Cipher*

- The Vigenère cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword.
- The method was originally described by Giovan Battista Bellaso in his 1553 however, the scheme was later misattributed to Blaise de Vigenère in the 19th century, and is now widely known as the "Vigenère cipher".

# *Operation*

- You start with the first letter of the text you want to encrypt.
- You add that letter to the first letter of your keyword.
- You then divide that by mod 26.
- Finally you move on to the next letter of both the text and the keyword.

# *Decryption*

- You start with the first letter of the text you want to decrypt.
- You subtract the first letter of your keyword from it.
- You then divide that by mod 26.
- Finally you move on to the next letter of both the text and the keyword.

# *Frequency Analysis*

- In cryptanalysis, frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext
- Frequency analysis is based on the fact that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies.
  - there is a characteristic distribution of letters that is roughly the same for almost all samples of that language

# *Frequency Analysis*

- For instance, given a section of English language, E, T, A and O are the most common, while Z, Q and X are rare.
- Likewise, TH, ER, ON, and AN are the most common common pairs of letters (termed bigrams or digraphs), and SS , EE , TT , and FF are the most common repeats.

# Example

- Suppose Eve has intercepted the cryptogram below, and it is known to be encrypted using a simple substitution cipher.

LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKYSTYLXZIXLIKIIXPIJVSZEYPERRGERIM

WQLMGLMXQERIWGPSRIHMXQEREKIETXMJTTPRGEVEKEITREWHEXXLEXXMZITWAWWSQWXSWEEXTVEPMRXRSJ

GSTVRIEYVIEXCVMUIMWERGMIWXMJMGCSMWXSJOMIQXLIVIQIVIXQSVSTWHKPEGARCSXRWIEVSWIIBXV

IZMXFSJXLIKEGAEWHEPSWYSWIWIEVXLISXLIVXLIRGEPHQIIVIBGIIHMWYPPFLEVHEWHYPSRRFQMXLE

PPXLIECCIEVEWGISJKTVWMRLIHYSPLIQLIQIMYLSXSJLIMWRIGXQEROIVFVIZEVAEKPIEWHXEAMWYEPP

- XLMWYRMWXSGSWRMHIVEXMSWMGSTPHLEVHPFKPEZINTCMXIVJSVLMRSCMWMSWVIRCIGXMWYMX

- Eve could use frequency analysis to help solve the message along the following lines: counts of the letters in the cryptogram show that I is the most common single letter, XL most common bigram, and XLI is the most common trigram.

# Continued

- e is the most common letter in the English language, th is the most common bigram, and the the most common trigram.
- This strongly suggests that X~t, L~h and I~e.
- The second most common letter in the cryptogram is E; since the first and second most frequent letters in the English language, e and t are accounted for,
  - Eve guesses that E~a (the third most frequent letter)
- Tentatively making these assumptions, the following partial decrypted message is obtained.

heVeTCSWPeYVaWHaVSReQMthaYVaOeaWHRtatePFaMVaWHKVSTYhtZetheKeetPeJVSZaYPaRRGaReM  
WQhMGhMtQaReWGPSReHMTQaRaKeaTtMJTPRGaVaKaeTRaWHatthattMZetWAWSQWtSWatTVaPMRtRSJ  
GSTVReaYVeatCVMUeMwARGMeWtMJMGCSMWtSJOMeQtheVeQeVetQSVSTWHKPaGARCStRWeaVSWeeBtV  
eZMtFSJtheKaGAaWHaPSWYSWeWeaVtheStheVtheRGaPeRQeVeeBGeeHMWYPFhaVHaWHYPSRRFQMtha  
PPtheaCCeaVaWGeSJKTVWMRheHYSPHtheQeMYhtSJtheMWRReGtQaROeVFVeZaVAaKPeaWHtaAMWYaPP  
thMWYRMWtSGSWRMHeVatMSWMGSTPHhaVHPFKPaZeNTCMteVJSVhMRSCMWMSWVeRCeGtMWYMt

# Continued

- Using these initial guesses, Eve can spot patterns that confirm her choices.
  - such as "that".
- Moreover, other patterns suggest further guesses.
  - "Rtate" might be "state", which would mean R~s.
  - "atthattMZe" could be guessed as "atthattime", yielding M~i and Z~m.
  - "heVe" might be "here", giving V~r.
- Filling in these guesses, Eve gets:

hereTCSWPeYraWHarSseQithaYraOeaWHstatePFairaWHKrstYhtmetheKeetPeJrSmaYPassGasei  
WQhiGhitQaseWGPSsseHitQasaKeaTtiJTPsGaraKaeTsaWHatthattimeTWAWSQWtSWatTraPistsSJ  
GSTrseaYreatCriUeiWasGieWtiJiGCSiWtSJOieQthereQeretQsrSTWHKPaGAsCStsWearSWeeBtr  
emitFSJtheKaGAaWHaPSWYSWeWeartheStherthesGaPesQereeBGeeHiWYPFharHaWHYPSssFQitha  
PPtheaCCearaWGeSJKTrWisheHYSPHtheQeiYhtSJtheiWseGtQasOerFremarAaKPeaWHtaAiWYaPP  
thiWYsiWtSGSWsiHeratiSWiGSTPHharHPFKPameNTCiterJSrhisSCiWiSWresCeGtiWYit

# Continued

- These guesses suggest still others
  - for example, "remarA" could be "remark", implying A~k) and so on,
- It is relatively straightforward to deduce the rest of the letters, eventually yielding the plaintext:

hereuponlegrandarosewithagraveandstatelyairandbroughtmethebeetlefromaglasscasei

nwhichitwasencloseditwasabeautifulscarabaeusandatthattimeunknown tonaturalistsof

courseagreatprizeinascientificpointofviewthereweretworoundblackspotsnearoneextr

emityofthebackandalongoneneartheotherthescaleswereexceedinglyhardandglossywitha

lltheappearanceofburnishedgoldtheweightoftheinsectwasveryremarkableandtakingall

thingsintoconsiderationicouldhardlyblamejupiterforhisopinionrespectingit

# *Continued*

- At this point, it would be a good idea for Eve to insert spaces and punctuation yielding the following:

Hereupon Legrand arose, with a grave and stately air, and brought me the beetle from a glass case in which it was enclosed. It was a beautiful scarabaeus, and, at that time, unknown to naturalists—of course a great prize in a scientific point of view. There were two round black spots near one extremity of the back, and a long one near the other. The scales were exceedingly hard and glossy, with all the appearance of burnished gold. The weight of the insect was very remarkable, and, taking all things into consideration, I could hardly blame Jupiter for his opinion respecting it.