



---

---

# MUPEC Workshop on Codebreaking

*27 March 2004*

Prof. Joshua Holden

<http://www.rose-hulman.edu/~holden/MUPEC>

Rose-Hulman Institute of Technology

# Cryptography

- The study of how to send secret messages by codes and ciphers
- Today: three different techniques of cryptography
  - Additive ciphers
  - Multiplicative ciphers
  - Hill ciphers

# Additive ciphers

- Go back at least as far as Julius Caesar
- Change each letter to a number:

|   |   |   |   |   |   |   |   |   |   |    |    |    |
|---|---|---|---|---|---|---|---|---|---|----|----|----|
| a | b | c | d | e | f | g | h | i | j | k  | l  | m  |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

|    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| n  | o  | p  | q  | r  | s  | t  | u  | v  | w  | x  | y  | z  |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

- “Key” is a number between 0 and 25.
- “Ciphertext” letter is “plaintext” letter plus key.
- Wrap around so that  $26 = 0$ ,  $27 = 1$ , etc.
- Subtract 26 if you need to.

# Example

- Key is 11

|    |   |   |    |   |    |    |   |   |    |   |   |   |    |
|----|---|---|----|---|----|----|---|---|----|---|---|---|----|
| m  | e | e | t  | a | t  | m  | i | d | n  | i | g | h | t  |
| 12 | 4 | 4 | 19 | 0 | 19 | 12 | 8 | 3 | 13 | 8 | 6 | 7 | 19 |

(add the key)

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 23 | 15 | 15 | 30 | 11 | 30 | 23 | 19 | 14 | 24 | 19 | 17 | 18 | 30 |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|

(subtract 26 if you need to)

|    |    |    |   |    |   |    |    |    |    |    |    |    |   |
|----|----|----|---|----|---|----|----|----|----|----|----|----|---|
| 23 | 15 | 15 | 4 | 11 | 4 | 23 | 19 | 14 | 24 | 19 | 17 | 18 | 4 |
| X  | P  | P  | E | L  | E | X  | T  | O  | Y  | T  | R  | S  | E |

# Exercises (1)

**Exercise** Encrypt the sentence: “I came, I saw, I conquered” using an additive cipher and a key of 3. (This is the key that Julius Caesar liked.) Use pencil and paper and maybe a calculator if you need one.

**Exercise** Now decrypt the sentence using the UWHMW software.

# Breaking an additive cipher

- How do you break an additive cipher?
- In typical English text the letter “e” occurs most often: about 13% of the time.
- So the most common letter in the ciphertext is *probably* (not certainly) “e”.
- Then we can subtract the plaintext from the ciphertext to get the key.

# Example

BPQAA MVBMV KMPIA AMDMZ ITMA

- The most common letter is “M” = 12. Plaintext “e” = 4, so probably the key is  $12 - 4 = 8$ .

# Exercises (2)

**Exercise** Finish decrypting the ciphertext  
BPQAA MVBMV KMPIA AMDMZ ITMA  
using the UWHMW software.

# Exercises (3)

**Exercise** Practice breaking ciphers 1-10 from the UWHMW software. Use the letter frequency function to guess the ciphertext for “e” and the additive attack function to get the key. (It may take several guesses to get the right key. You will know it’s right when you get English words.) Then use the additive decrypt function to decipher the message.

Note: Pay special attention to the form of the decrypted message! The four digit number you need in the competition will be given to you in this same form.

# Affine ciphers

- There's nothing too special about addition — we can multiply as well.  
(Be careful: Multiplying by an even number is bad because you only get even ciphertext letters. So is multiplying by 13, because you only get multiples of 13. We call these “bad keys”.)
- We can do both: affine ciphers have two keys.
- Key  $a$  is for multiplying and key  $b$  is for adding.
- Ciphertext =  $a$  times plaintext plus  $b$

# Example

•  $a = 9, b = 3$

|   |    |    |    |   |    |   |   |   |    |   |   |    |    |
|---|----|----|----|---|----|---|---|---|----|---|---|----|----|
| f | u  | n  | w  | i | t  | h | c | i | p  | h | e | r  | s  |
| 5 | 20 | 13 | 22 | 8 | 19 | 7 | 2 | 8 | 15 | 7 | 4 | 17 | 18 |

(multiply by  $a$  and add  $b$ )

|    |     |     |     |    |     |    |    |    |     |    |    |     |     |
|----|-----|-----|-----|----|-----|----|----|----|-----|----|----|-----|-----|
| 48 | 183 | 120 | 201 | 75 | 174 | 66 | 21 | 75 | 138 | 66 | 39 | 156 | 165 |
|----|-----|-----|-----|----|-----|----|----|----|-----|----|----|-----|-----|

(subtract 26 as often as you need to)

|    |   |    |    |    |    |    |    |    |   |    |    |   |   |
|----|---|----|----|----|----|----|----|----|---|----|----|---|---|
| 22 | 1 | 16 | 19 | 23 | 18 | 14 | 21 | 23 | 8 | 14 | 13 | 0 | 9 |
| W  | B | Q  | T  | X  | S  | O  | V  | X  | I | O  | N  | A | J |

# Exercises (4)

**Exercise** Encrypt the sentence: “Every dog has its day” using an affine cipher with  $a = 3$ ,  $b = 2$ . Use pencil and paper and maybe a calculator if you need one.

**Exercise** Now decrypt the sentence using the UWHMW software.

# Breaking an affine cipher

- How do you break an affine cipher?
- In typical English text the letter “t” occurs second-most often: about 9% of the time.
- So the second-most common letter in the ciphertext is *probably* (not certainly) “t”. (Several other letters are very close!)
- If we know the ciphertext letters for “e” = 4 and “t” = 19 then we can set up two equations in two unknowns and find the key.

# Exercises (5)

**Exercise** Practice breaking ciphers 11-20 from the UWHMW software. Use the letter frequency function to guess the ciphertexts for “e” and “t” and the affine attack function to get the key. (It may take several guesses to get the right key. You will know it’s right when you get English words.) Then use the affine decrypt function to decipher the message.

# Hill ciphers

- Hill ciphers were invented in 1929 to defeat this sort of “letter frequency analysis”.
- The ciphertext is divided into “blocks” of two (or more) letters.
- The key is a 2 by 2 (or larger) matrix.  
(Be careful: Hill ciphers also have some “bad keys”, for example if all of the entries of the matrix are even.)

# Example

- Key is  $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

|   |   |    |    |   |    |   |   |    |   |    |    |
|---|---|----|----|---|----|---|---|----|---|----|----|
| c | a | t  | s  | a | n  | d | d | o  | g | s  | x  |
| 2 | 0 | 19 | 18 | 0 | 13 | 3 | 3 | 14 | 6 | 18 | 23 |

- $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$ , and so on.

|   |   |    |    |   |    |   |   |    |   |    |    |
|---|---|----|----|---|----|---|---|----|---|----|----|
| c | a | t  | s  | a | n  | d | d | o  | g | s  | x  |
| 2 | 0 | 19 | 18 | 0 | 13 | 3 | 3 | 14 | 6 | 18 | 23 |

(multiply the matrix by the vector)

|   |   |    |    |    |    |   |   |   |    |    |    |
|---|---|----|----|----|----|---|---|---|----|----|----|
| 0 | 2 | 18 | 37 | 13 | 13 | 3 | 6 | 6 | 20 | 23 | 41 |
|---|---|----|----|----|----|---|---|---|----|----|----|

(subtract 26 as often as you need to)

|   |   |    |    |    |    |   |   |   |    |    |    |
|---|---|----|----|----|----|---|---|---|----|----|----|
| 0 | 2 | 18 | 11 | 13 | 13 | 3 | 6 | 6 | 20 | 23 | 15 |
| A | C | S  | L  | N  | N  | D | G | G | U  | X  | P  |

# Exercises (6)

**Exercise** Encrypt the phrase: “Jack and Jill” using an affine cipher with key  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ . Use pencil and paper and maybe a calculator if you need one.

**Exercise** Now decrypt the phrase using the UWHMW software. Enter the key into the software from left to right and top to bottom.

# Breaking a Hill cipher

- How do you break a Hill cipher?
- Notice that the same letter doesn't always get encrypted the same way!
- Need to count “digraphs” — two-letter blocks.
- The most common is “th”. The second most common is “he”. But there are many digraphs that are very close to the same frequency!
- Once we know ciphertext for “th” and “he” we can set up four equations in four unknowns to find the key.

# Exercises (7)

**Exercise** Find the key and decrypt the following (ungrammatical and probably false) sentence: “OVKCPI TCKCOV YUZVZG XKSOPH MFPICQ TBOVNN SPJFOO LUOVRR XXNYHH IQPITC FKKT” using the UWMHW software.

# Exercises (8)

**Exercise** Practice breaking ciphers 21-30 from the UWHMW software. Use the digraph frequency function to guess the ciphertexts for “th” and “he” and the Hill attack function to get the key. (It may take many guesses to get the right key. You will know it’s right when you get English words.) Then use the Hill decrypt function to decipher the message.

Hint for cipher 21: plaintext “he” = ciphertext “jx”

# Letter to number table

|   |   |   |   |   |   |   |   |   |   |    |    |    |
|---|---|---|---|---|---|---|---|---|---|----|----|----|
| a | b | c | d | e | f | g | h | i | j | k  | l  | m  |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

|    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| n  | o  | p  | q  | r  | s  | t  | u  | v  | w  | x  | y  | z  |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |