## Simple Codes

MTH 440

## Not all codes are for the purpose of secrecy

- Morse Code
- ASCII
- Zip codes
- Area codes
- Library book codes
- Credit Cards...



## ASCII Code



Source: www.LookupTables.com

## Steganography: Hidden in plain

sight
(example from
http://www.bbc.co.uk/news/10
480477)

Logos 2

Examples of steganography

## Example 1: Coded message

Apparently neutral's protest is thoroughly discounted and ignored.
Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.
Take second letter of each word to get message:
Pershing sails from NY June 1
Example 2: Coded images: Least Significant Bits (LSB) insertion Original image

Altered image


Areas where binary code of pixel has been altered

Binary code from original image pixel 1
100000001010010010110101101101011111001110110111111001111011001100110000 Changes made on altered image pixel $\mathbb{1}$
100000011010010010110100101101001111001010110110111001101011001100110011
Read last digit:
1000001 which is ASCII binary code for $\left.\frac{A}{[1]} \overline{2}\right] \frac{3}{3} \overline{4}$

## Permutation Ciphers

- The plaintext is all there, it is just mixed up in some way.
- Scytale
- Block and Rotate
- Transposition Ciphers:
- Columnar Transposition


## Columnar Transposition

- The secret "key" is the width of a rectangle
- The message is written across the rectangle and the ciphertext is read down the columns:

Plaintext: The answers to the test are abcbbadeac Rectangle width: 7

| 1 | $\mathbf{2}$ | $\mathbf{3}$ | $\mathbf{4}$ | $\mathbf{5}$ | 6 | 7 |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| T | H | E | A | N | S | W |
| E | R | S | T | O | T | H |
| E | T | E | S | T | A | R |
| E | A | B | C | B | B | A |
| D | E | A | C | X | X | X |

Ciphertext: TEEEDHRTAEESEBAATSCCNOTBXSTABXWHRAX

Plaintext: The answers to the test are abcbbadeac Rectangle width: 7

|  |  |  |  |  |  |  |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- |

Ciphertext: TEEEDHRTAEESEBAATSCCNOTBXSTABXWHRAX

Plaintext: The answers to the test are abcbbadeac Rectangle width: 7

|  |  |  |  |  |  |  |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- |

Ciphertext: TEEEDHRTAEESEBAATSCCNOTBSTABWHRA

## Your turn - decipher the following (width = 11; no padding)

keonamoklwsilbseutdtegwneissspd

## Width unknown

- DECRYPT: (Assume rows were not permuted.)

TOQOIEOUTOEHFUFDQTAHTETATEUHREESHRHSAEE HNUEEEILSOYUMSSSSTQFPS
Guess the number of rows/columns \& check (there are online applets for this)

- OR Look:

TOQOIEOUTOEHFUFDQTAHTETATEUHREESHRHSAEE HNUEEEILSOYUMSSSSTQFPS
TOQOIEOUTOEHFUFDQTAHTETATEUHREESHRHSAEE HNUEEEILSOYUMSSSSTQFPS

## COLUMNAR transposition

TOQOIEOUTOEHFUFDQTAHTETATEUHREESHRHSAEEHNUEEE ILSOYUMSSSSTQFPS

|  |  |  |  |  |  |  |  |  |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |

We either have 5 full rows or 4 full rows and one partial row. There are 61 letters. Since 61 is not divisible by 5 we have 4 full rows and a partial. $61=4 \times 15+1$. So we have 4 rows of 15 columns and the last row just has one column

## COLUMNAR transposition

- TOQOIEOUTOEHFUFDQTAHTETATEUHREESHRHS AEEHNUEEEILSOYUMSSSSTQFPS

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1 | 1 | 1 | 1 | 1 | 1 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| T | E | O | U | T | E | E | E | R | E | U | I | Y | S | Q |
| O | O | E | F | A | T | U | E | H | E | E | L | U | S | F |
| Q | U | H | D | H | A | H | S | S | H | E | S | M | S | P |
| O | T | F | Q | T | T | R | H | A | N | E | O | S | T | S |
| I |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

- This doesn’t look promising


## COLUMNAR transposition

## TOQOIEOUTOEHFUFDQTAHTETATEUHREESHRHS AEEHNUEEEILSOYUMSSSSTQFPS

|  |  |  |  |  |  |
| :--- | :--- | :--- | :--- | :--- | :--- |
| T | H |  |  |  |  |
| O | F |  |  |  |  |
| Q | U |  |  |  |  |
| O |  |  |  |  |  |
| I |  |  |  |  |  |
| E |  |  |  |  |  |
| O |  |  |  |  |  |
| U |  |  |  |  |  |
| T |  |  |  |  |  |
| O |  |  |  |  |  |
| E |  |  |  |  |  |

So we have 11 full rows or 10 full rows and one partial row. Since 61 is not divisible by 11 we have 10 full rows and one partial:

$$
61=10 \times 6+1
$$

So if this is correct, we have 6 columns.

## COLUMNAR transposition

## TOQOIEOUTOEHFUFDQTAHTETATEUHREESHRHS AEEHNUEEEILSOYUMSSSSTQFPS

| 1 | 2 | 3 | 4 | 5 | 6 |
| :---: | :---: | :---: | :---: | :---: | :---: |
| T | H | E | S | U | M |
| O | F | T | H | E | S |
| Q | U | A | R | E | S |
| O | F | T | H | E | S |
| I | D | E | S | I | S |
| E | Q | U | A | L | T |
| O | T | H | E | S | Q |
| U | A | R | E | O | F |
| T | H | E | H | Y | P |
| O | T | E | N | U | S |
| E |  |  |  |  |  |

## To easy? Add a codeword and "alphabetize" the columns

| P | Y | T | H | A | G |
| :---: | :---: | :---: | :---: | :---: | :---: |
| T | H | E | S | U | M |
| O | F | T | H | E | S |
| Q | U | A | R | E | S |
| O | F | T | H | E | S |
| I | D | E | S | I | S |
| E | Q | U | A | L | T |
| O | T | H | E | S | Q |
| U | A | R | E | O | F |
| T | H | E | H | Y | P |
| O | T | E | N | U | S |
| E |  |  |  |  |  |


| A | G | H | P | T | Y |
| :---: | :---: | :---: | :---: | :---: | :---: |
| U | M | S | T | E | H |
| E | S | H | O | T | F |
| E | S | R | Q | A | U |
| E | S | H | O | T | F |
| I | S | S | I | E | D |
| L | T | A | E | U | Q |
| S | Q | E | O | H | T |
| O | F | E | U | R | A |
| Y | P | H | T | E | H |
| U | S | N | O | E | T |
|  |  |  | E |  |  |

Ciphertext: ueeeilsoyumsssstqfpsshrhsaeehntoqoieoutoeetateuhreehfufdqtaht

## Simple Substitution Ciphers

- Substitute each letter by another letter or symbol


## PigPen cipher

| A | B | C |  |  |  |
| :--- | :--- | :--- | :--- | :--- | :--- |
| D | E | F |  | J | K |
|  | L | N | $\bullet$ |  |  |
| G | H | I |  | P | $\bullet$ |
|  | $\bullet$ | R |  |  |  |



## Back Jacket Cover of Dan Brown's The Lost Symbol



## Too easy? Add a codeword

Codeword "Davinci" (don’t use repeated letters, followed by unused letters alphabetically)

| $D$ | $A$ | $V$ |
| :---: | :---: | :---: |
| I | $N$ | $C$ |
| $B$ | $E$ | $F$ |



## Decrypt（homework）－what is the codeword and plaintext？

$$
\begin{aligned}
& \text { L. ヨフVロ フロフレレロコ } \\
& \text { ココフコ VロトVワロ 」 リヲワ } \\
& \text { 以下セヒロコ 」コワコく「へ } \\
& \text { 〈ワレ・, VロFV・ロ」レन・フ }
\end{aligned}
$$

$$
\begin{aligned}
& \text { コケ」 く・ケへ คフ・ロ ココロ円 } \\
& \text { ・ロロ? }
\end{aligned}
$$

## Breaking simple substitution ciphers

- Frequency analysis:

Most common English letters: ETAOINSHRDLU
Most common double letters: SS, EE, TT, FF, LL, MM, OO Most common digraphs: th er on an re he in ed nd ha at en es of or nt ea ti to it st io le is ou ar as de rt ve Single letter words: A, I

- http://www.wiley.com/college/mat/gilbert139343/java Lava11 s.html


## Polybuis Checkerboard

|  | 1 | 2 | 3 | 4 | 5 |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 1 | A | B | C | D | E |
| 2 | F | G | H | I/J | K |
| 3 | L | M | N | O | P |
| 4 | Q | R | S | T | U |
| 5 | V | W | X | Y | Z |

Decipher: 2315313134

## Polybuis Checkerboard with codeword

|  | 1 | 2 | 3 | 4 | 5 |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 1 | M | A | T | H | E |
| 2 | I/J | C | S | B | D |
| 3 | F | G | K | L | N |
| 4 | O | P | Q | R | U |
| 5 | V | W | X | Y | Z |

Homework: Encipher "Mathematics is fun" using the codeword "Cryptology"

## Playfair Cipher - pairs of letter are enciphered together

| 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 |

Encipher: I am brilliant
Decipher: zdtxptbqcz

## Playfair Cipher - mix up the letters (code word or pattern)

| A | Q | $P$ | $O$ | $N$ |
| :---: | :---: | :---: | :---: | :---: |
| B | R | $Y$ | $X$ | $M$ |
| C | S | $Z$ | $W$ | $L$ |
| D | T | U | V | K |
| E | F | G | $H$ | $I / J$ |

Write the grid for the playfair cipher using the codeword "Wendesday" then encrypt "Tuesday"

