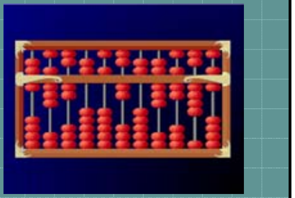
Ones and Zeros

Chapter 12

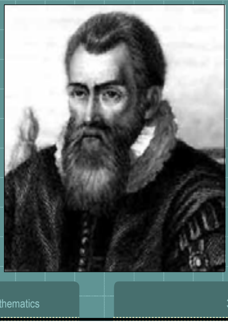
Early Computers

- The definition of a computer is “a device that computes, …”
- The abacus could be considered the first computer.
- Its effectiveness has withstood the test of time and it is still used in some parts of the world.



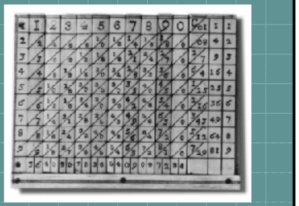
John Napier (1550 - 1617)

- In 1617, Scottish mathematician John Napier invented a technique of using numbering rods for multiplication.
- The rods became known as "*Napier's Bones*."



Napier’s Bones

- Napier's Bones were multiplication tables inscribed on strips of wood or bone.
- Napier’s idea led to the invention of the slide rule in the mid 1600s by William Oughtred.

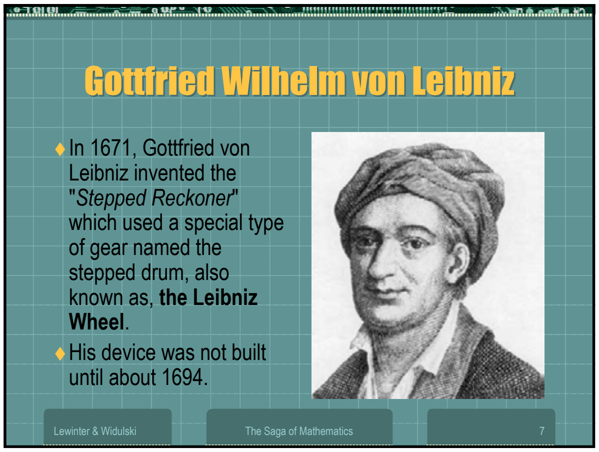


The Pascaline

- In 1642, Blaise Pascal invented his "Pascaline" calculator.
- Pascal, a mathematician and philosopher, and his father, a tax official, were compiling tax reports for the French government in Paris.

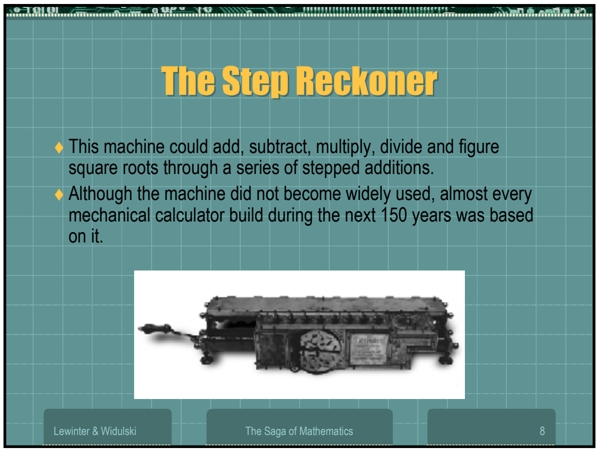
The Pascaline

- As they agonized over the columns of figures, Pascal decided to build a machine that would do the job much faster and more accurately.
- His machine could add and subtract.
- The machine used a series of toothed wheels, which were turned by hand and which could handle numbers up to 999,999.999.
- Pascal’s device was also called the “numerical calculator” and was one of the world’s first mechanical adding machines.



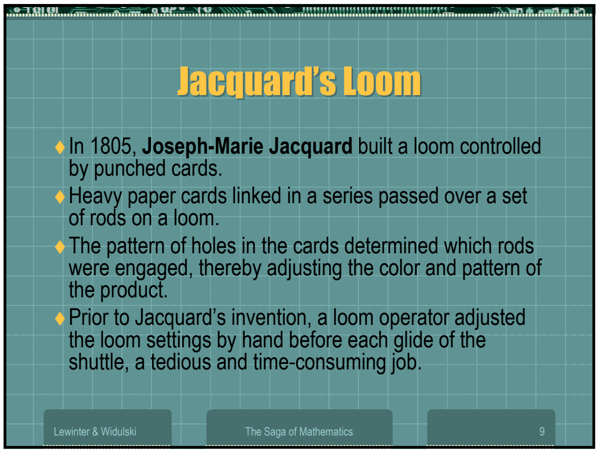
Gottfried Wilhelm von Leibniz

- In 1671, Gottfried von Leibniz invented the "*Stepped Reckoner*" which used a special type of gear named the stepped drum, also known as, **the Leibniz Wheel**.
- His device was not built until about 1694.



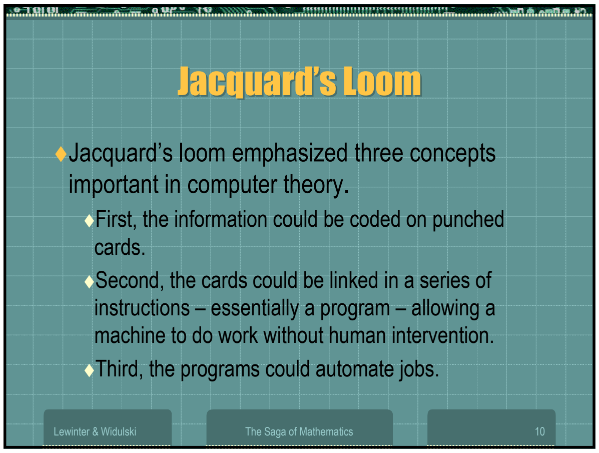
The Step Reckoner

- This machine could add, subtract, multiply, divide and figure square roots through a series of stepped additions.
- Although the machine did not become widely used, almost every mechanical calculator build during the next 150 years was based on it.



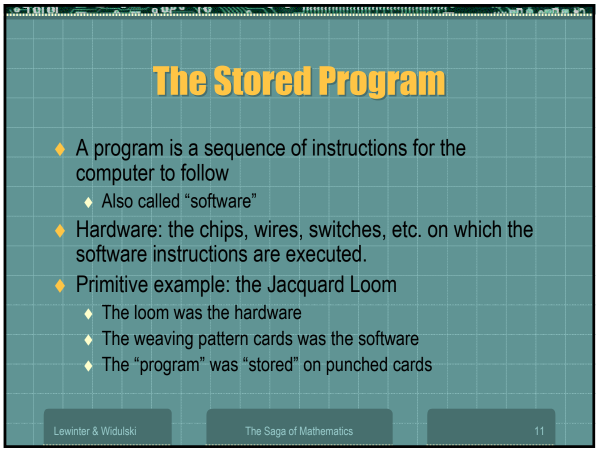
Jacquard's Loom

- In 1805, **Joseph-Marie Jacquard** built a loom controlled by punched cards.
- Heavy paper cards linked in a series passed over a set of rods on a loom.
- The pattern of holes in the cards determined which rods were engaged, thereby adjusting the color and pattern of the product.
- Prior to Jacquard's invention, a loom operator adjusted the loom settings by hand before each glide of the shuttle, a tedious and time-consuming job.



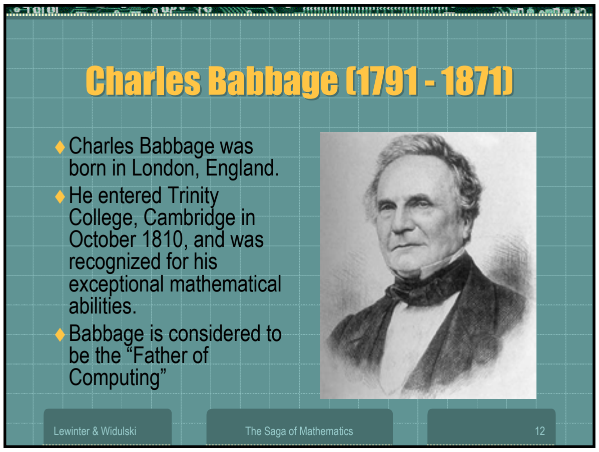
Jacquard's Loom

- Jacquard's loom emphasized three concepts important in computer theory.
  - First, the information could be coded on punched cards.
  - Second, the cards could be linked in a series of instructions – essentially a program – allowing a machine to do work without human intervention.
  - Third, the programs could automate jobs.



The Stored Program

- A program is a sequence of instructions for the computer to follow
  - Also called “software”
- Hardware: the chips, wires, switches, etc. on which the software instructions are executed.
- Primitive example: the Jacquard Loom
  - The loom was the hardware
  - The weaving pattern cards was the software
  - The “program” was “stored” on punched cards



Charles Babbage (1791 - 1871)

- Charles Babbage was born in London, England.
- He entered Trinity College, Cambridge in October 1810, and was recognized for his exceptional mathematical abilities.
- Babbage is considered to be the “Father of Computing”

Charles Babbage (1791 - 1871)

- In 1827 Babbage became Lucasian Professor of Mathematics at Cambridge, a position he held for 12 years, although he never taught.
- He had become engrossed in the main passion of his life – the development of a mechanical computer.
- Babbage began to construct a small difference engine in 1819 and had completed it by 1822.
- Babbage illustrated what his small engine was capable of doing by calculating successive terms of the sequence $n^2 + n + 41$.

Charles Babbage (1791 - 1871)

- On 13 July 1823 Babbage received a gold medal from the Astronomical Society for his development of the difference engine.
- By 1834 Babbage had completed the first drawings of the analytical engine, the forerunner of the modern electronic computer.
- Babbage discussed the concept of using punched cards to control the operation of his calculating machine, but he was never able to build a full working model.

Charles Babbage (1791 - 1871)

- Babbage's ideas embodied five key concepts of modern computers:
  1. Input device
  2. Processor or number calculator
  3. Control unit to direct the task to be performed and the sequence of calculations.
  4. Storage place to hold number waiting to be processed
  5. Output device

Charles Babbage (1791 - 1871)

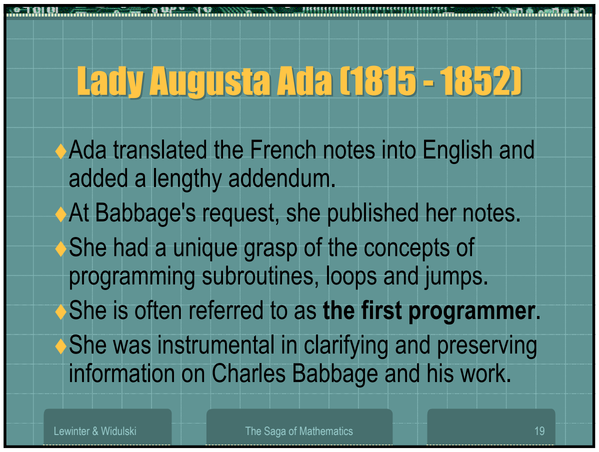
- Although Babbage died before he could construct his machine, such a computer has been built following Babbage's own design criteria.
- In 1834 Babbage published his most influential work *On the Economy of Machinery and Manufactures*, in which he proposed an early form of what today we call **operations research**.

Lady Augusta Ada (1815 - 1852)

- Augusta Ada was the daughter of the poet, Lord Byron.
- Her mother encouraged her to study mathematics and music.
- She was a bright mathematician who was introduced to Charles Babbage in 1833.

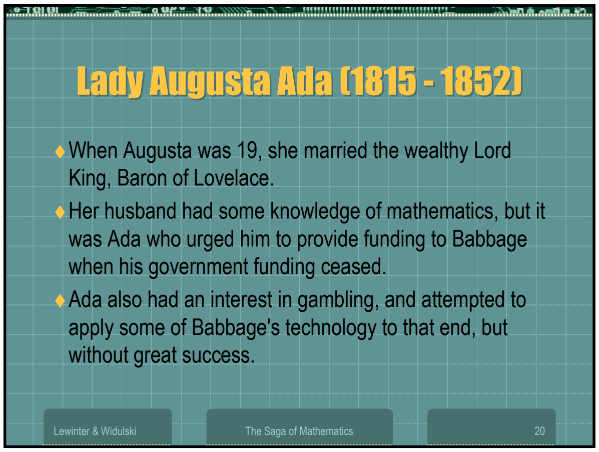
Lady Augusta Ada (1815 - 1852)

- Ada Byron was fascinated by a demonstration of Babbage's Difference Engine.
- Babbage found that Ada understood and could explain the workings of his machine better than anyone else.
- Babbage later toured Europe giving lectures on his more advanced concept, the Analytical Engine, a machine which he never fully constructed.
- Extensive notes were taken of some of these lectures in French.



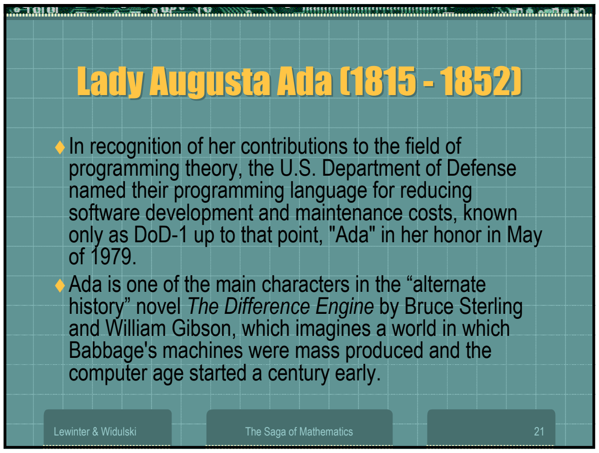
Lady Augusta Ada (1815 - 1852)

- Ada translated the French notes into English and added a lengthy addendum.
- At Babbage's request, she published her notes.
- She had a unique grasp of the concepts of programming subroutines, loops and jumps.
- She is often referred to as **the first programmer**.
- She was instrumental in clarifying and preserving information on Charles Babbage and his work.



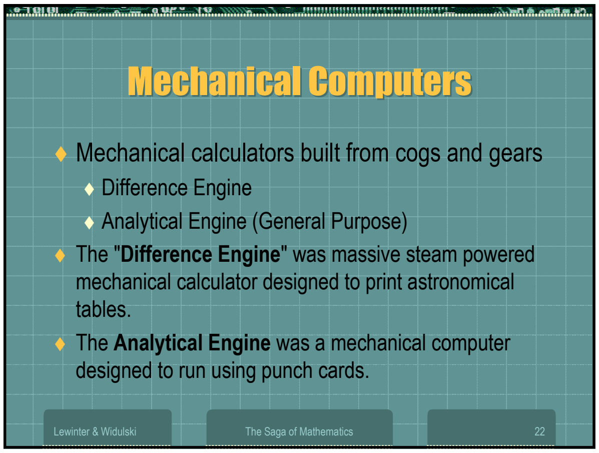
Lady Augusta Ada (1815 - 1852)

- When Augusta was 19, she married the wealthy Lord King, Baron of Lovelace.
- Her husband had some knowledge of mathematics, but it was Ada who urged him to provide funding to Babbage when his government funding ceased.
- Ada also had an interest in gambling, and attempted to apply some of Babbage's technology to that end, but without great success.



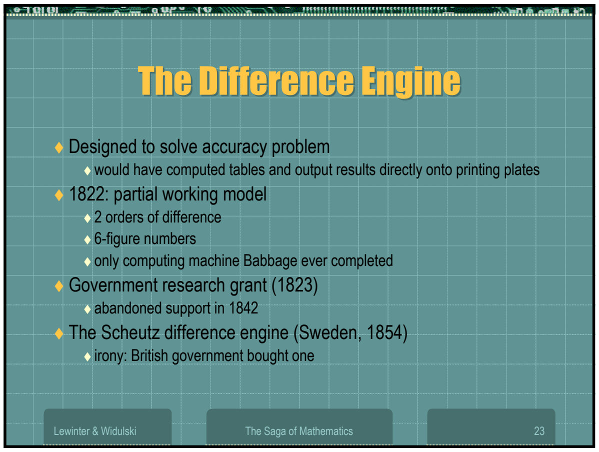
Lady Augusta Ada (1815 - 1852)

- In recognition of her contributions to the field of programming theory, the U.S. Department of Defense named their programming language for reducing software development and maintenance costs, known only as DoD-1 up to that point, "Ada" in her honor in May of 1979.
- Ada is one of the main characters in the “alternate history” novel *The Difference Engine* by Bruce Sterling and William Gibson, which imagines a world in which Babbage's machines were mass produced and the computer age started a century early.



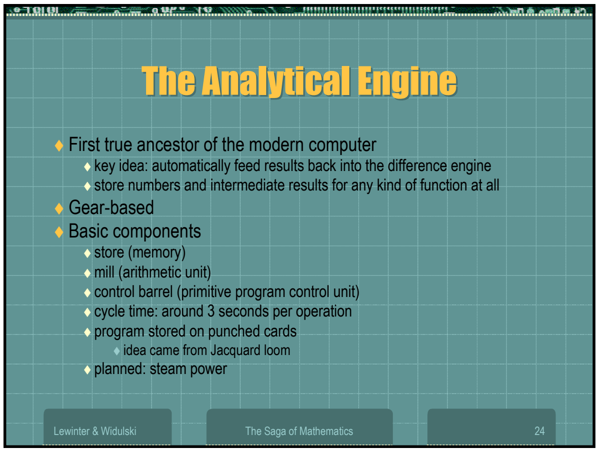
Mechanical Computers

- Mechanical calculators built from cogs and gears
  - Difference Engine
  - Analytical Engine (General Purpose)
- The "**Difference Engine**" was massive steam powered mechanical calculator designed to print astronomical tables.
- The **Analytical Engine** was a mechanical computer designed to run using punch cards.



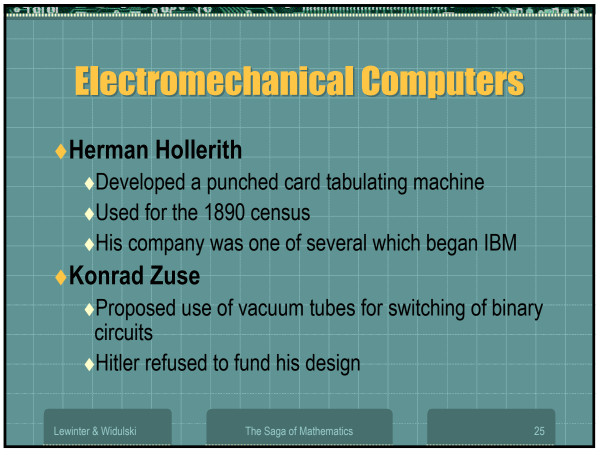
The Difference Engine

- Designed to solve accuracy problem
  - would have computed tables and output results directly onto printing plates
- 1822: partial working model
  - 2 orders of difference
  - 6-figure numbers
  - only computing machine Babbage ever completed
- Government research grant (1823)
  - abandoned support in 1842
- The Scheutz difference engine (Sweden, 1854)
  - irony: British government bought one



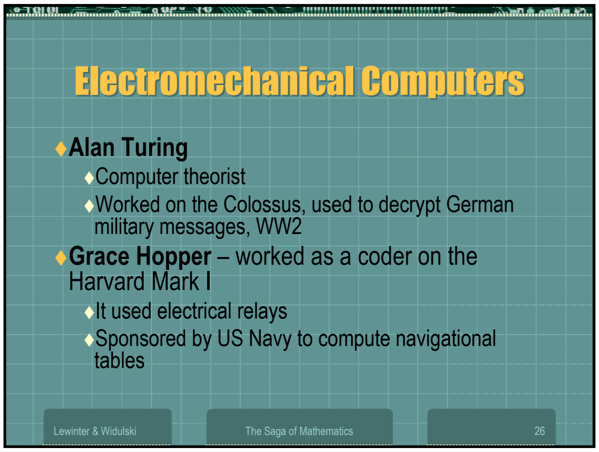
The Analytical Engine

- First true ancestor of the modern computer
  - key idea: automatically feed results back into the difference engine
  - store numbers and intermediate results for any kind of function at all
- Gear-based
- Basic components
  - store (memory)
  - mill (arithmetic unit)
  - control barrel (primitive program control unit)
  - cycle time: around 3 seconds per operation
  - program stored on punched cards
    - idea came from Jacquard loom
  - planned: steam power



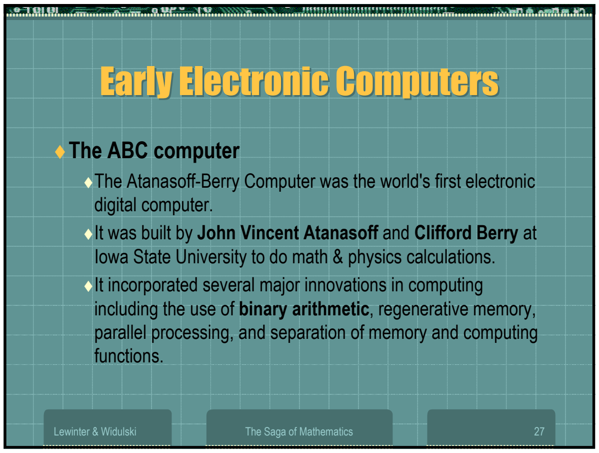
Electromechanical Computers

- **Herman Hollerith**
  - Developed a punched card tabulating machine
  - Used for the 1890 census
  - His company was one of several which began IBM
- **Konrad Zuse**
  - Proposed use of vacuum tubes for switching of binary circuits
  - Hitler refused to fund his design



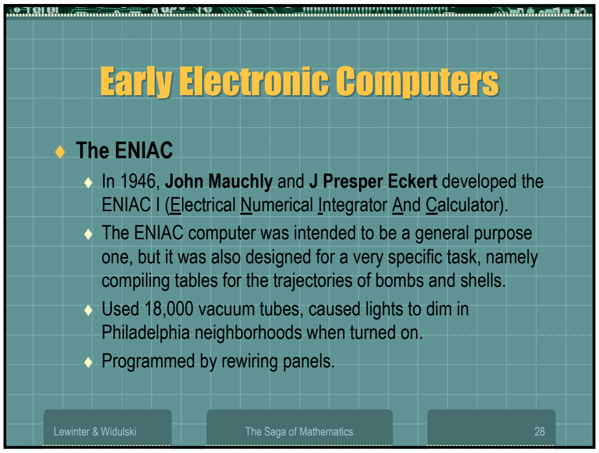
Electromechanical Computers

- **Alan Turing**
  - Computer theorist
  - Worked on the Colossus, used to decrypt German military messages, WW2
- **Grace Hopper** – worked as a coder on the Harvard Mark I
  - It used electrical relays
  - Sponsored by US Navy to compute navigational tables



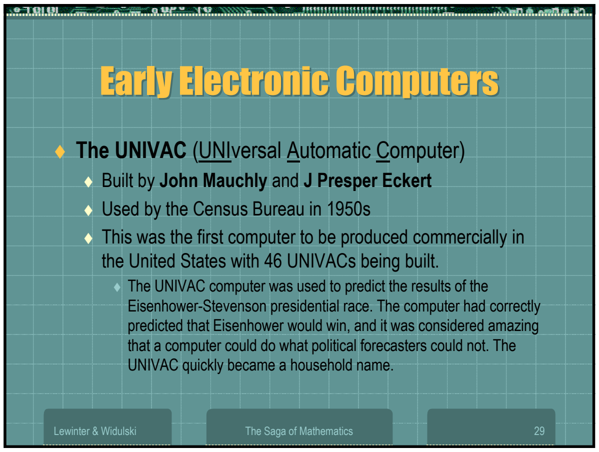
Early Electronic Computers

- **The ABC computer**
  - The Atanasoff-Berry Computer was the world's first electronic digital computer.
  - It was built by **John Vincent Atanasoff** and **Clifford Berry** at Iowa State University to do math & physics calculations.
  - It incorporated several major innovations in computing including the use of **binary arithmetic**, regenerative memory, parallel processing, and separation of memory and computing functions.



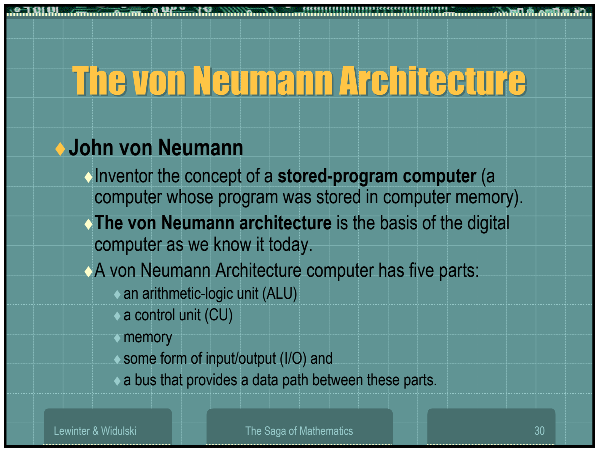
Early Electronic Computers

- **The ENIAC**
  - In 1946, **John Mauchly** and **J Presper Eckert** developed the ENIAC I (Electrical Numerical Integrator And Calculator).
  - The ENIAC computer was intended to be a general purpose one, but it was also designed for a very specific task, namely compiling tables for the trajectories of bombs and shells.
  - Used 18,000 vacuum tubes, caused lights to dim in Philadelphia neighborhoods when turned on.
  - Programmed by rewiring panels.



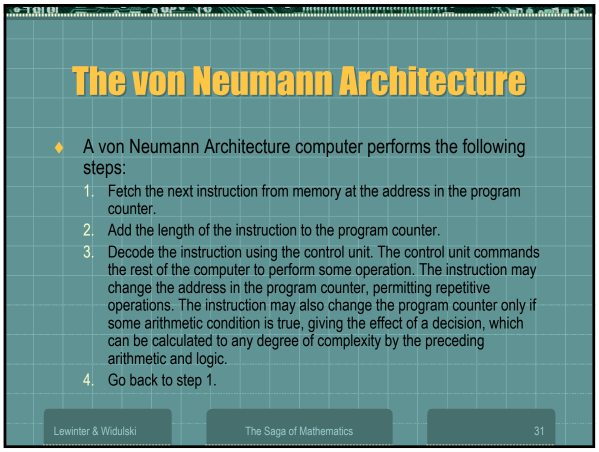
Early Electronic Computers

- **The UNIVAC** (UNIversal Automatic Computer)
  - Built by **John Mauchly** and **J Presper Eckert**
  - Used by the Census Bureau in 1950s
  - This was the first computer to be produced commercially in the United States with 46 UNIVACs being built.
    - The UNIVAC computer was used to predict the results of the Eisenhower-Stevenson presidential race. The computer had correctly predicted that Eisenhower would win, and it was considered amazing that a computer could do what political forecasters could not. The UNIVAC quickly became a household name.



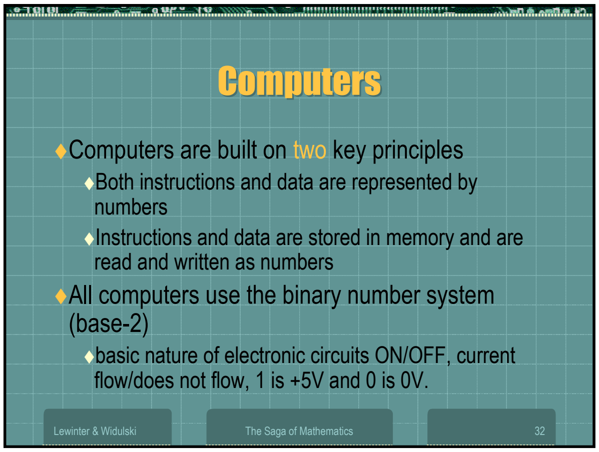
The von Neumann Architecture

- **John von Neumann**
  - Inventor the concept of a **stored-program computer** (a computer whose program was stored in computer memory).
  - **The von Neumann architecture** is the basis of the digital computer as we know it today.
  - A von Neumann Architecture computer has five parts:
    - an arithmetic-logic unit (ALU)
    - a control unit (CU)
    - memory
    - some form of input/output (I/O) and
    - a bus that provides a data path between these parts.



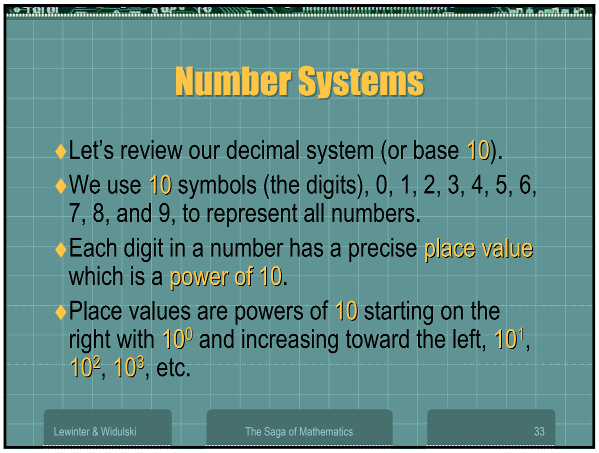
The von Neumann Architecture

- A von Neumann Architecture computer performs the following steps:
  1. Fetch the next instruction from memory at the address in the program counter.
  2. Add the length of the instruction to the program counter.
  3. Decode the instruction using the control unit. The control unit commands the rest of the computer to perform some operation. The instruction may change the address in the program counter, permitting repetitive operations. The instruction may also change the program counter only if some arithmetic condition is true, giving the effect of a decision, which can be calculated to any degree of complexity by the preceding arithmetic and logic.
  4. Go back to step 1.



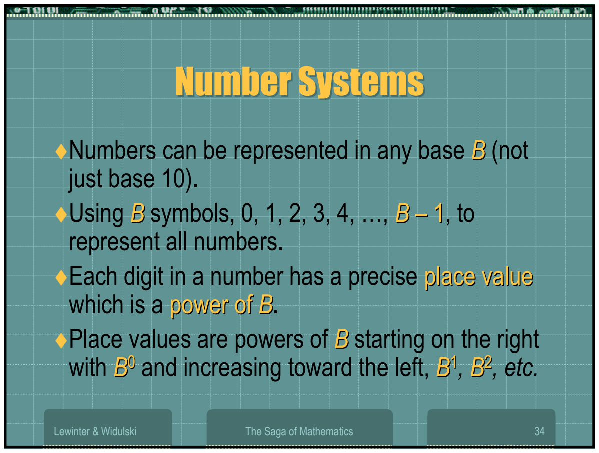
Computers

- Computers are built on two key principles
  - Both instructions and data are represented by numbers
  - Instructions and data are stored in memory and are read and written as numbers
- All computers use the binary number system (base-2)
  - basic nature of electronic circuits ON/OFF, current flow/does not flow, 1 is +5V and 0 is 0V.



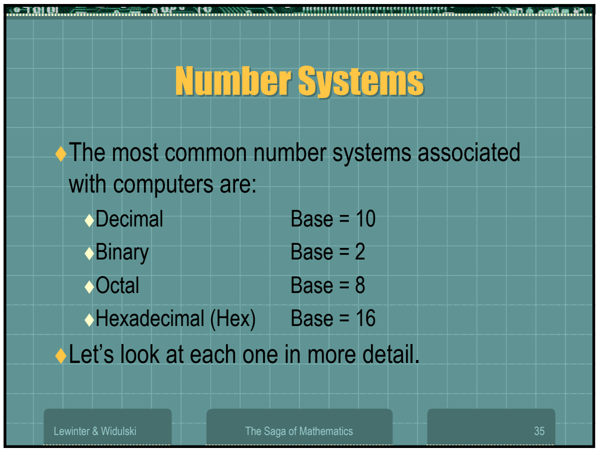
Number Systems

- Let's review our decimal system (or base 10).
- We use 10 symbols (the digits), 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9, to represent all numbers.
- Each digit in a number has a precise place value which is a power of 10.
- Place values are powers of 10 starting on the right with 10^0 and increasing toward the left, 10^1, 10^2, 10^3, etc.



Number Systems

- Numbers can be represented in any base *B* (not just base 10).
- Using *B* symbols, 0, 1, 2, 3, 4, …, *B* – 1, to represent all numbers.
- Each digit in a number has a precise place value which is a power of *B*.
- Place values are powers of *B* starting on the right with B^0 and increasing toward the left, B^1, B^2, *etc.*

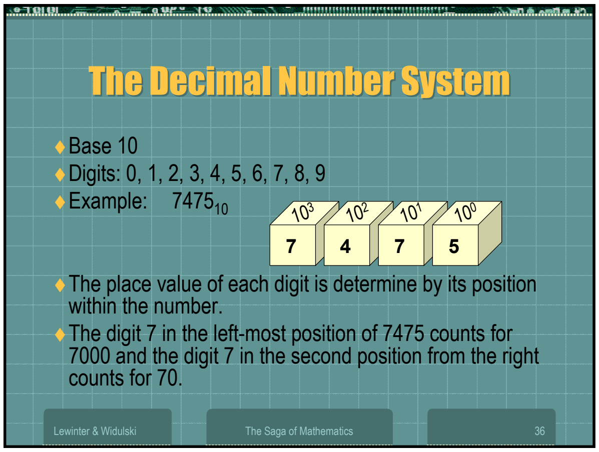


Number Systems

- The most common number systems associated with computers are:

Decimal	Base = 10
Binary	Base = 2
Octal	Base = 8
Hexadecimal (Hex)	Base = 16

- Let's look at each one in more detail.

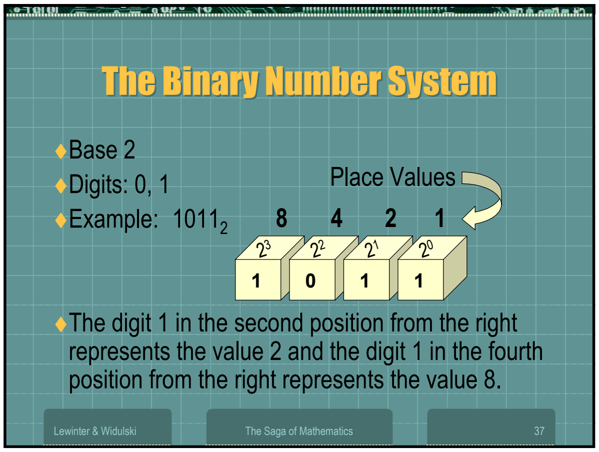


The Decimal Number System

- Base 10
- Digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
- Example: 7475_{10}

10^3	10^2	10^1	10^0
7	4	7	5

- The place value of each digit is determine by its position within the number.
- The digit 7 in the left-most position of 7475 counts for 7000 and the digit 7 in the second position from the right counts for 70.



The Binary Number System

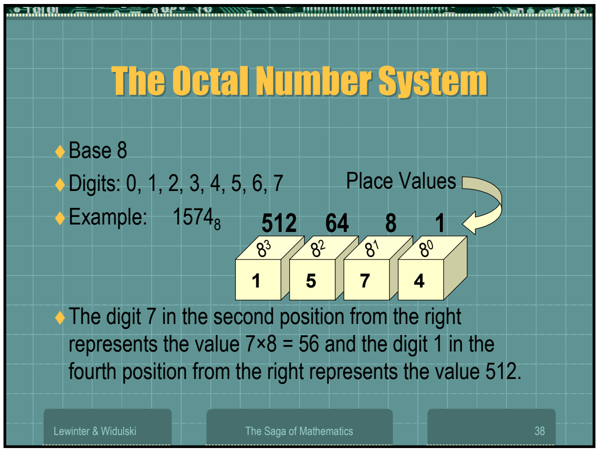
- Base 2
- Digits: 0, 1
- Example: 1011_2

Place Values

8	4	2	1
2^3	2^2	2^1	2^0
1	0	1	1

- The digit 1 in the second position from the right represents the value 2 and the digit 1 in the fourth position from the right represents the value 8.

Lewinter & Widulski The Saga of Mathematics 37



The Octal Number System

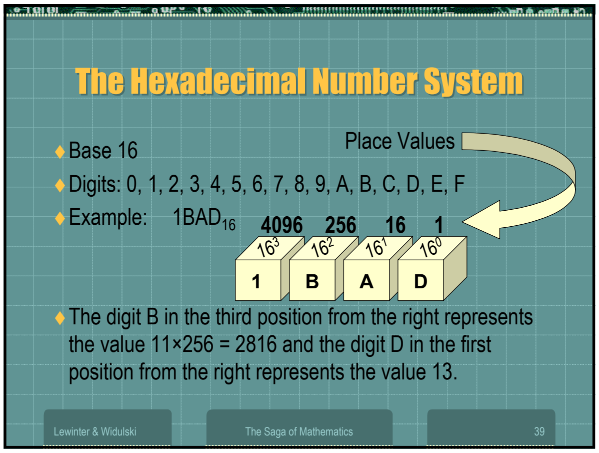
- Base 8
- Digits: 0, 1, 2, 3, 4, 5, 6, 7
- Example: 1574_8

Place Values

512	64	8	1
8^3	8^2	8^1	8^0
1	5	7	4

- The digit 7 in the second position from the right represents the value 7×8 = 56 and the digit 1 in the fourth position from the right represents the value 512.

Lewinter & Widulski The Saga of Mathematics 38



The Hexadecimal Number System

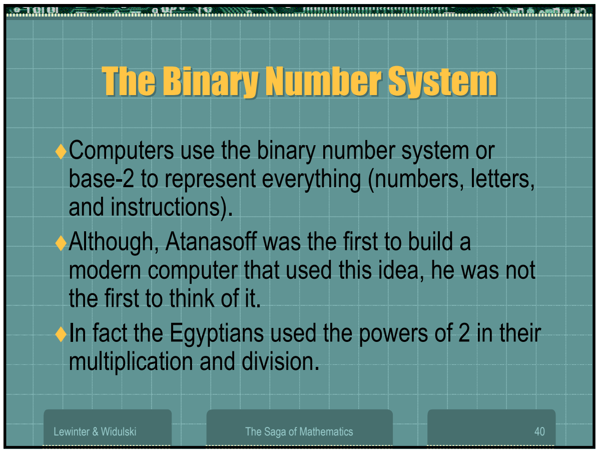
- Base 16
- Digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
- Example: $1BAD_{16}$

Place Values

4096	256	16	1
16^3	16^2	16^1	16^0
1	B	A	D

- The digit B in the third position from the right represents the value 11×256 = 2816 and the digit D in the first position from the right represents the value 13.

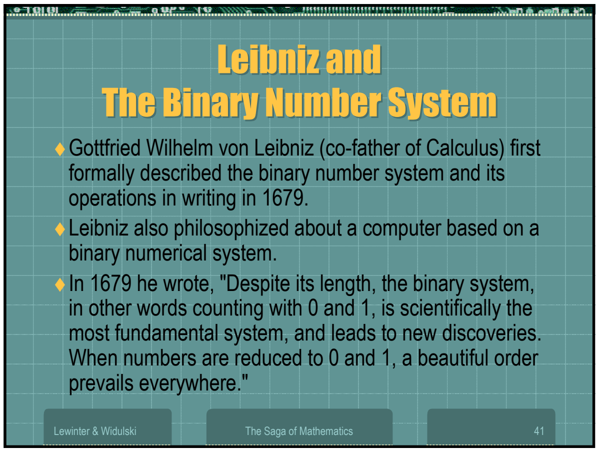
Lewinter & Widulski The Saga of Mathematics 39



The Binary Number System

- Computers use the binary number system or base-2 to represent everything (numbers, letters, and instructions).
- Although, Atanasoff was the first to build a modern computer that used this idea, he was not the first to think of it.
- In fact the Egyptians used the powers of 2 in their multiplication and division.

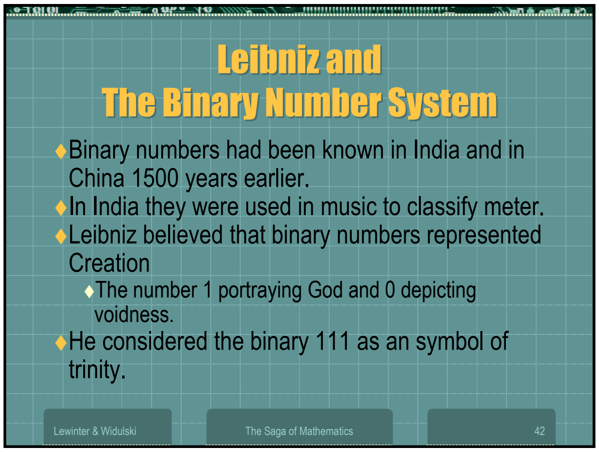
Lewinter & Widulski The Saga of Mathematics 40



Leibniz and The Binary Number System

- Gottfried Wilhelm von Leibniz (co-father of Calculus) first formally described the binary number system and its operations in writing in 1679.
- Leibniz also philosophized about a computer based on a binary numerical system.
- In 1679 he wrote, "Despite its length, the binary system, in other words counting with 0 and 1, is scientifically the most fundamental system, and leads to new discoveries. When numbers are reduced to 0 and 1, a beautiful order prevails everywhere."

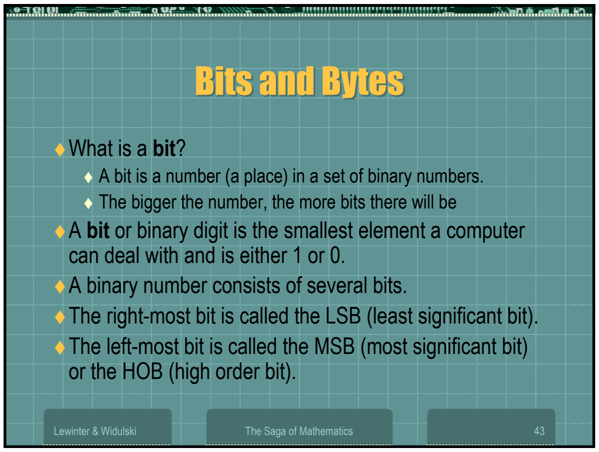
Lewinter & Widulski The Saga of Mathematics 41



Leibniz and The Binary Number System

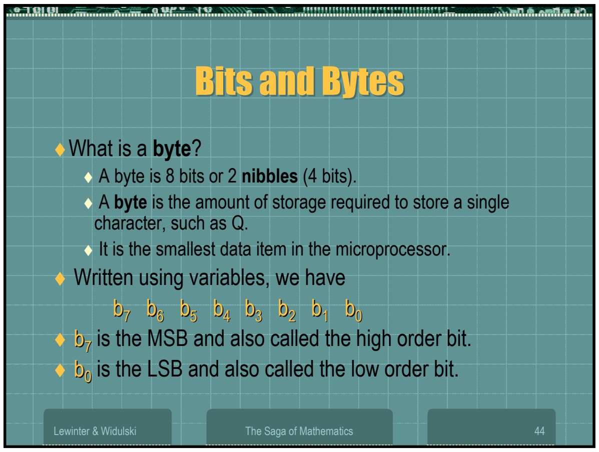
- Binary numbers had been known in India and in China 1500 years earlier.
- In India they were used in music to classify meter.
- Leibniz believed that binary numbers represented Creation
  - The number 1 portraying God and 0 depicting voidness.
- He considered the binary 111 as an symbol of trinity.

Lewinter & Widulski The Saga of Mathematics 42



Bits and Bytes

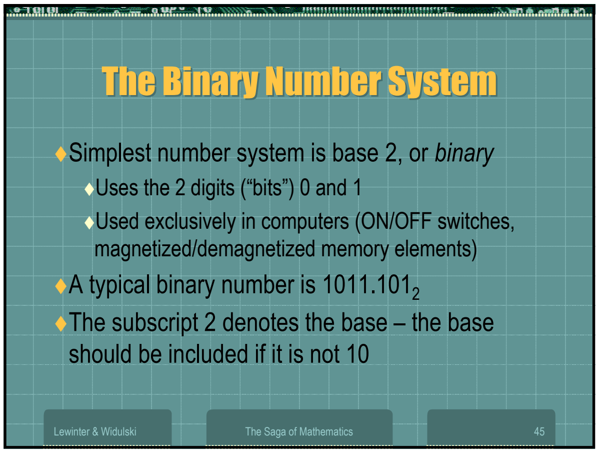
- What is a **bit**?
  - A bit is a number (a place) in a set of binary numbers.
  - The bigger the number, the more bits there will be
- A **bit** or binary digit is the smallest element a computer can deal with and is either 1 or 0.
- A binary number consists of several bits.
- The right-most bit is called the LSB (least significant bit).
- The left-most bit is called the MSB (most significant bit) or the HOB (high order bit).



Bits and Bytes

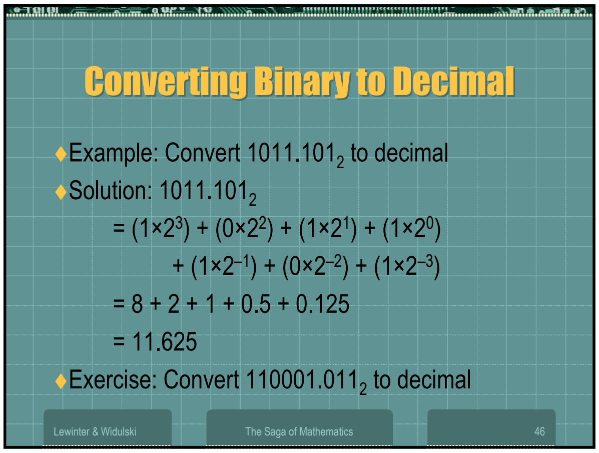
- What is a **byte**?
  - A byte is 8 bits or 2 **nibbles** (4 bits).
  - A **byte** is the amount of storage required to store a single character, such as Q.
  - It is the smallest data item in the microprocessor.
- Written using variables, we have

  b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0
- b_7 is the MSB and also called the high order bit.
- b_0 is the LSB and also called the low order bit.



The Binary Number System

- Simplest number system is base 2, or *binary*
  - Uses the 2 digits ("bits") 0 and 1
  - Used exclusively in computers (ON/OFF switches, magnetized/demagnetized memory elements)
- A typical binary number is 1011.101_2
- The subscript 2 denotes the base – the base should be included if it is not 10



Converting Binary to Decimal

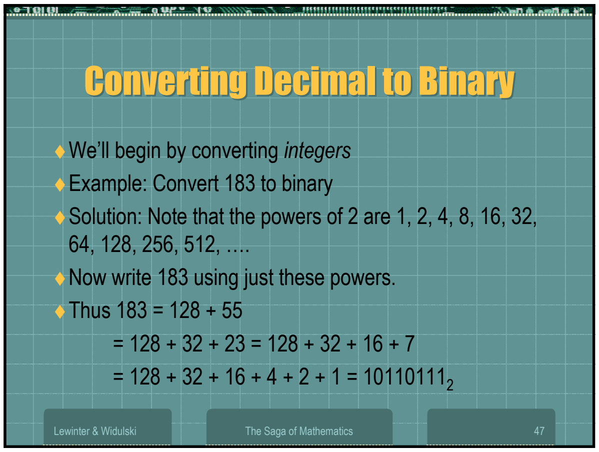
- Example: Convert 1011.101_2 to decimal
- Solution: 1011.101_2

  $= (1\times2^3) + (0\times2^2) + (1\times2^1) + (1\times2^0)$

  $+ (1\times2^{-1}) + (0\times2^{-2}) + (1\times2^{-3})$

  $= 8 + 2 + 1 + 0.5 + 0.125$

  $= 11.625$
- Exercise: Convert 110001.011_2 to decimal

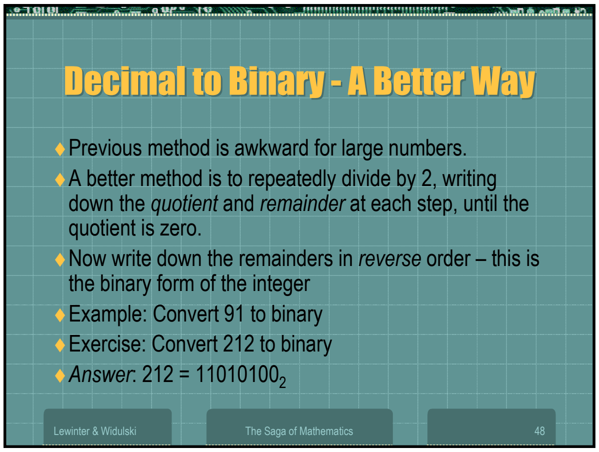


Converting Decimal to Binary

- We'll begin by converting *integers*
- Example: Convert 183 to binary
- Solution: Note that the powers of 2 are 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, ….
- Now write 183 using just these powers.
- Thus $183 = 128 + 55$

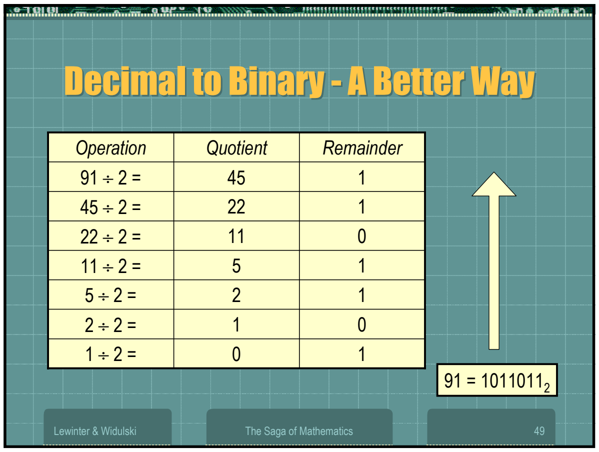
  $= 128 + 32 + 23 = 128 + 32 + 16 + 7$

  $= 128 + 32 + 16 + 4 + 2 + 1 = 10110111_2$



Decimal to Binary - A Better Way

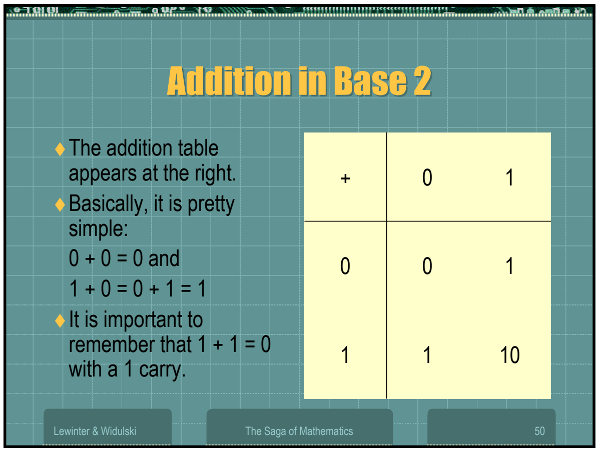
- Previous method is awkward for large numbers.
- A better method is to repeatedly divide by 2, writing down the *quotient* and *remainder* at each step, until the quotient is zero.
- Now write down the remainders in *reverse* order – this is the binary form of the integer
- Example: Convert 91 to binary
- Exercise: Convert 212 to binary
- *Answer*: $212 = 11010100_2$



Decimal to Binary - A Better Way

Operation	Quotient	Remainder
91 ÷ 2 =	45	1
45 ÷ 2 =	22	1
22 ÷ 2 =	11	0
11 ÷ 2 =	5	1
5 ÷ 2 =	2	1
2 ÷ 2 =	1	0
1 ÷ 2 =	0	1

$91 = 1011011_2$



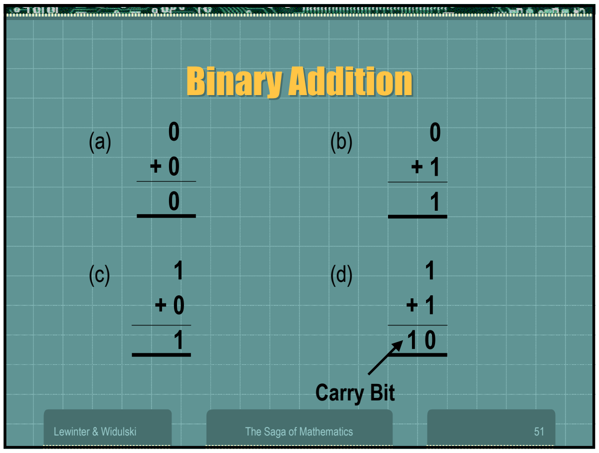
Addition in Base 2

- The addition table appears at the right.
- Basically, it is pretty simple:

  0 + 0 = 0 and

  1 + 0 = 0 + 1 = 1
- It is important to remember that 1 + 1 = 0 with a 1 carry.

+	0	1
0	0	1
1	1	10



Binary Addition

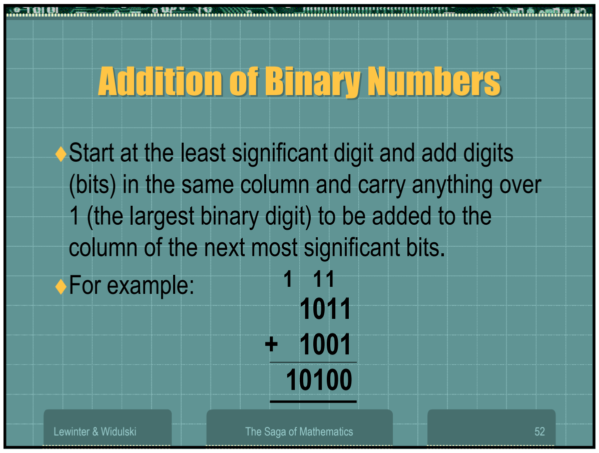
(a) $$\begin{array}{r} 0 \\ +\,0 \\ \hline 0 \end{array}$$

(b) $$\begin{array}{r} 0 \\ +\,1 \\ \hline 1 \end{array}$$

(c) $$\begin{array}{r} 1 \\ +\,0 \\ \hline 1 \end{array}$$

(d) $$\begin{array}{r} 1 \\ +\,1 \\ \hline 1\,0 \end{array}$$

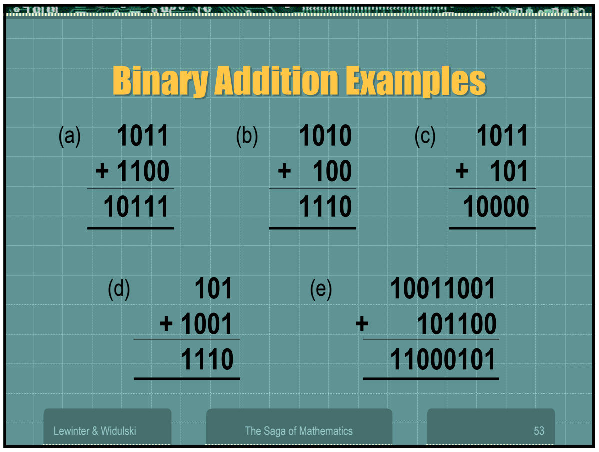
Carry Bit



Addition of Binary Numbers

- Start at the least significant digit and add digits (bits) in the same column and carry anything over 1 (the largest binary digit) to be added to the column of the next most significant bits.
- For example:

$$\begin{array}{r} 1\ \ \ 11\ \ \\ 1011 \\ +\ \ 1001 \\ \hline 10100 \end{array}$$



Binary Addition Examples

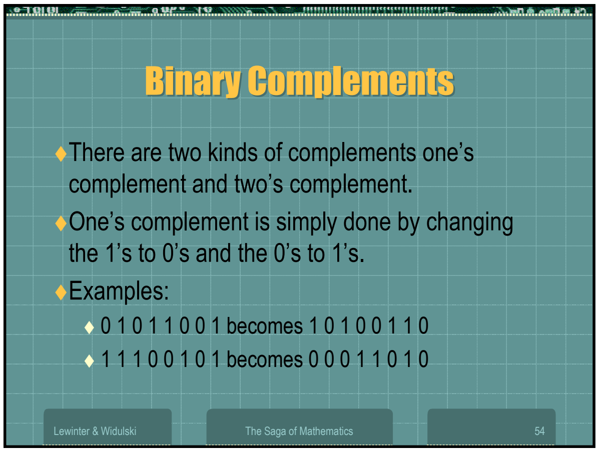
(a) $$\begin{array}{r} 1011 \\ +\,1100 \\ \hline 10111 \end{array}$$

(b) $$\begin{array}{r} 1010 \\ +\ \ 100 \\ \hline 1110 \end{array}$$

(c) $$\begin{array}{r} 1011 \\ +\ \ 101 \\ \hline 10000 \end{array}$$

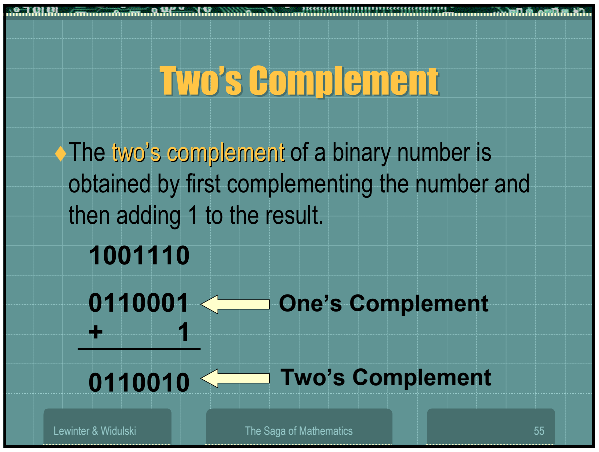
(d) $$\begin{array}{r} 101 \\ +\,1001 \\ \hline 1110 \end{array}$$

(e) $$\begin{array}{r} 10011001 \\ +\ \ \ 101100 \\ \hline 11000101 \end{array}$$



Binary Complements

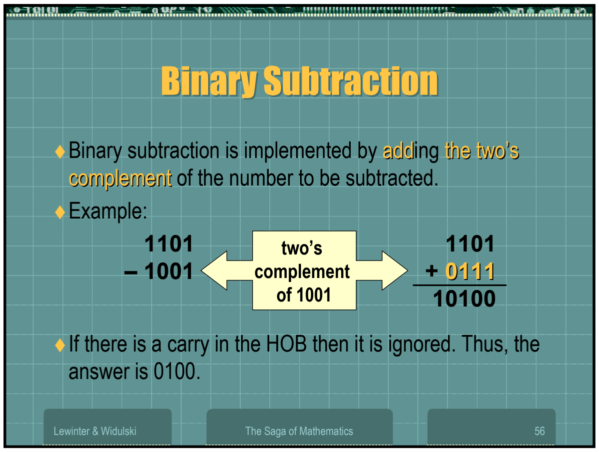
- There are two kinds of complements one’s complement and two’s complement.
- One’s complement is simply done by changing the 1’s to 0’s and the 0’s to 1’s.
- Examples:
  - 0 1 0 1 1 0 0 1 becomes 1 0 1 0 0 1 1 0
  - 1 1 1 0 0 1 0 1 becomes 0 0 0 1 1 0 1 0



Two's Complement

- The two's complement of a binary number is obtained by first complementing the number and then adding 1 to the result.

```
1001110

0110001  <——  One's Complement
+      1
-------
0110010  <——  Two's Complement
```

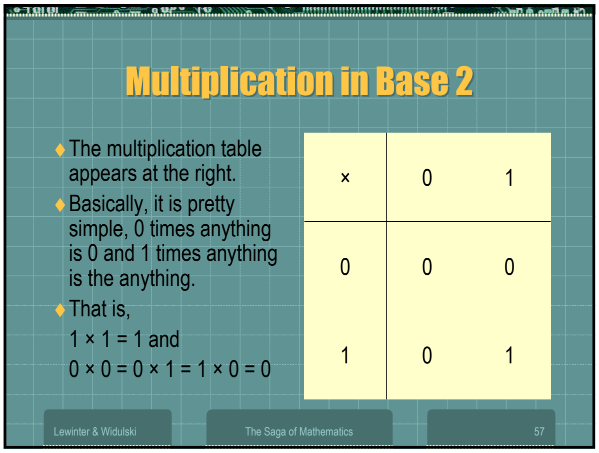


Binary Subtraction

- Binary subtraction is implemented by adding the two's complement of the number to be subtracted.
- Example:

```
  1101          two's            1101
– 1001   <——  complement  ——>  + 0111
                of 1001        ------
                                10100
```

- If there is a carry in the HOB then it is ignored. Thus, the answer is 0100.



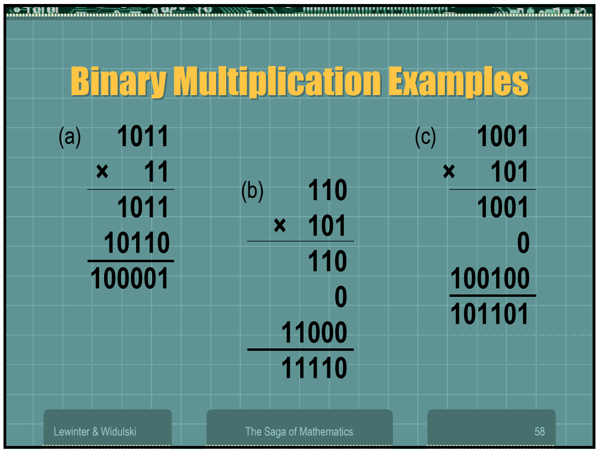
Multiplication in Base 2

- The multiplication table appears at the right.
- Basically, it is pretty simple, 0 times anything is 0 and 1 times anything is the anything.
- That is,

  1 × 1 = 1 and

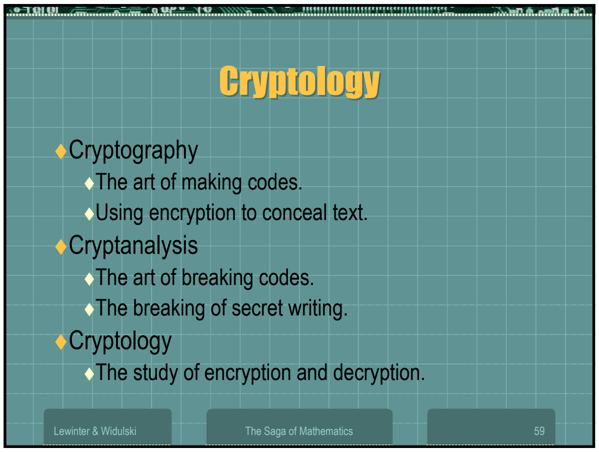
  0 × 0 = 0 × 1 = 1 × 0 = 0

×	0	1
0	0	0
1	0	1



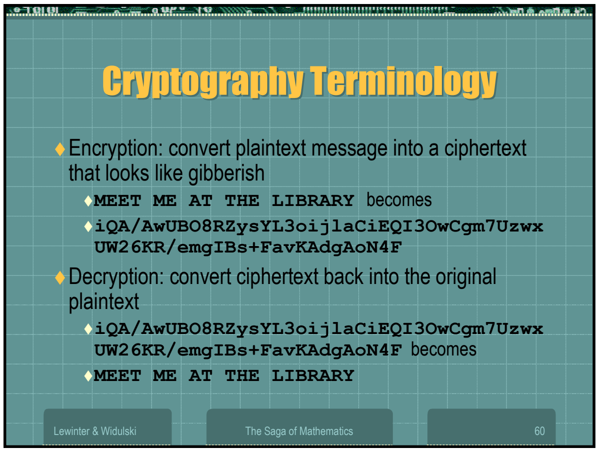
Binary Multiplication Examples

```
(a)   1011                           (c)   1001
    ×   11                                × 101
    ------          (b)    110            ------
      1011               × 101              1001
     10110               -----                 0
    ------                 110            100100
    100001                   0            ------
                         11000            101101
                         -----
                         11110
```



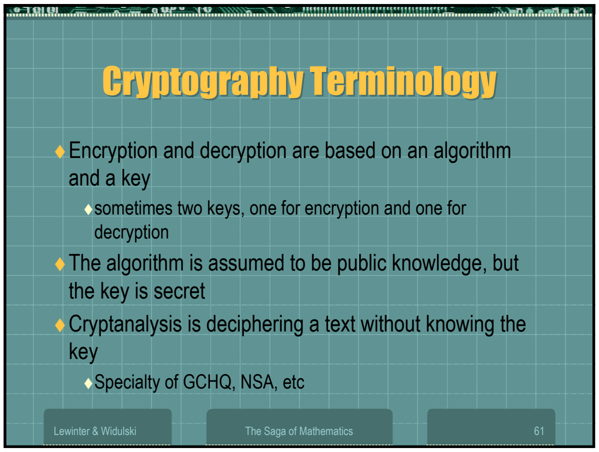
Cryptology

- Cryptography
  - The art of making codes.
  - Using encryption to conceal text.
- Cryptanalysis
  - The art of breaking codes.
  - The breaking of secret writing.
- Cryptology
  - The study of encryption and decryption.



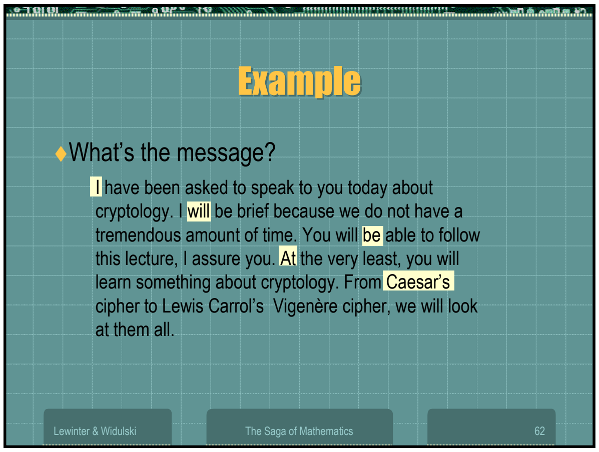
Cryptography Terminology

- Encryption: convert plaintext message into a ciphertext that looks like gibberish
  - **`MEET ME AT THE LIBRARY`** becomes
  - **`iQA/AwUBO8RZysYL3oijlaCiEQI3OwCgm7Uzwx UW26KR/emgIBs+FavKAdgAoN4F`**
- Decryption: convert ciphertext back into the original plaintext
  - **`iQA/AwUBO8RZysYL3oijlaCiEQI3OwCgm7Uzwx UW26KR/emgIBs+FavKAdgAoN4F`** becomes
  - **`MEET ME AT THE LIBRARY`**



Cryptography Terminology

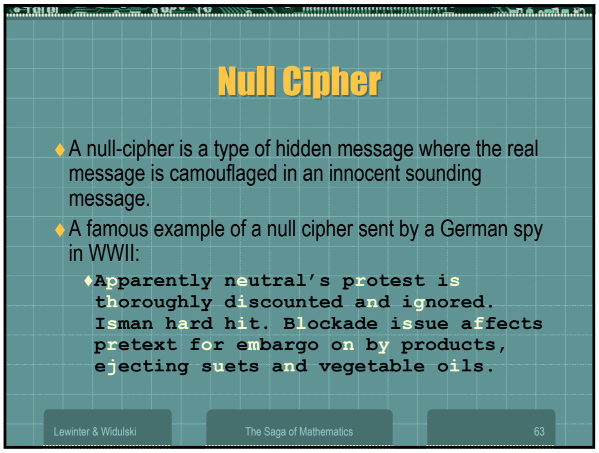
- Encryption and decryption are based on an algorithm and a key
  - sometimes two keys, one for encryption and one for decryption
- The algorithm is assumed to be public knowledge, but the key is secret
- Cryptanalysis is deciphering a text without knowing the key
  - Specialty of GCHQ, NSA, etc



Example

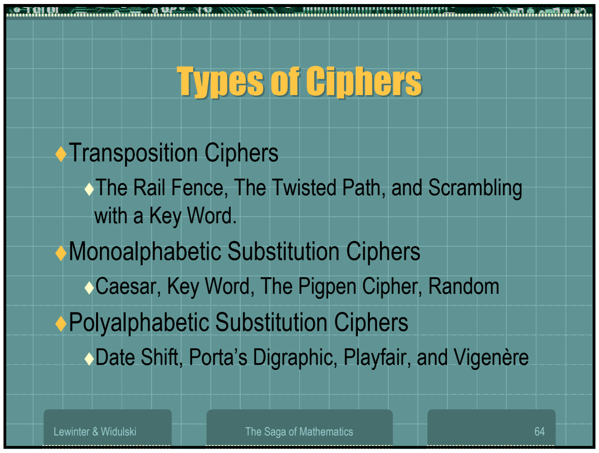
- What's the message?

  I have been asked to speak to you today about cryptology. I will be brief because we do not have a tremendous amount of time. You will be able to follow this lecture, I assure you. At the very least, you will learn something about cryptology. From Caesar's cipher to Lewis Carrol's Vigenère cipher, we will look at them all.



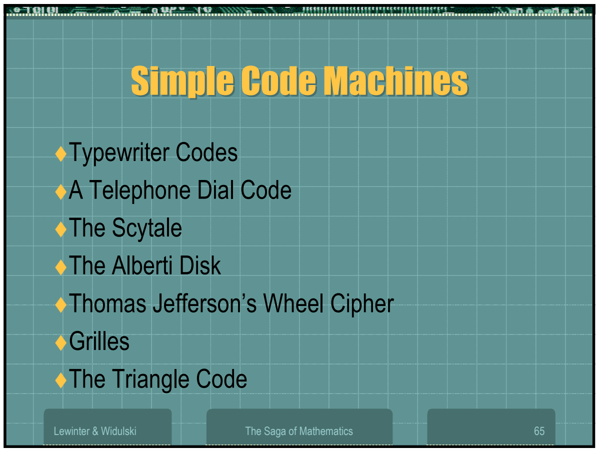
Null Cipher

- A null-cipher is a type of hidden message where the real message is camouflaged in an innocent sounding message.
- A famous example of a null cipher sent by a German spy in WWII:
  - `Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.`



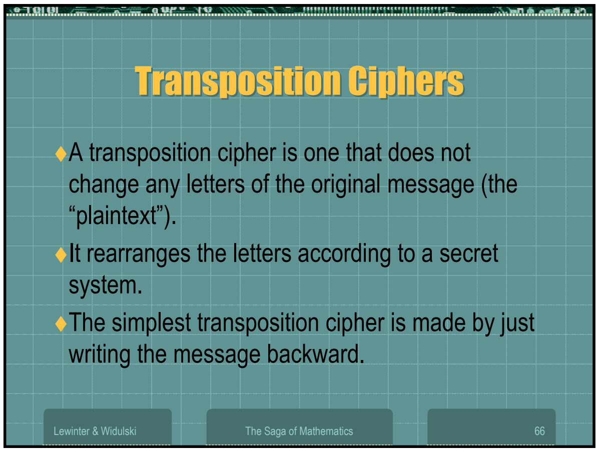
Types of Ciphers

- Transposition Ciphers
  - The Rail Fence, The Twisted Path, and Scrambling with a Key Word.
- Monoalphabetic Substitution Ciphers
  - Caesar, Key Word, The Pigpen Cipher, Random
- Polyalphabetic Substitution Ciphers
  - Date Shift, Porta's Digraphic, Playfair, and Vigenère



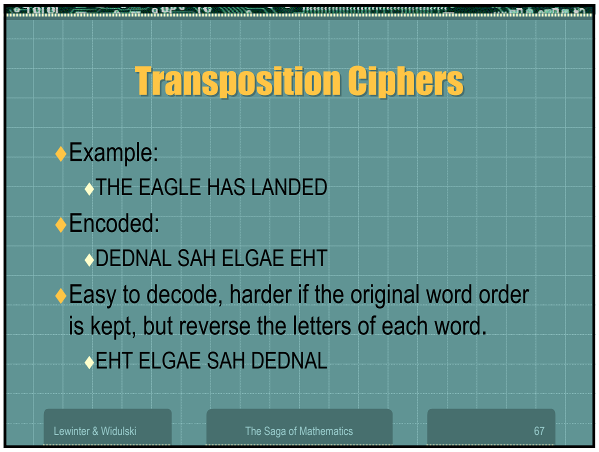
Simple Code Machines

- Typewriter Codes
- A Telephone Dial Code
- The Scytale
- The Alberti Disk
- Thomas Jefferson's Wheel Cipher
- Grilles
- The Triangle Code



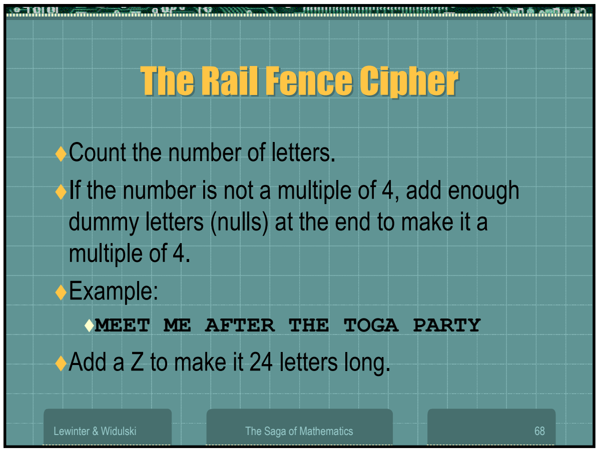
Transposition Ciphers

- A transposition cipher is one that does not change any letters of the original message (the "plaintext").
- It rearranges the letters according to a secret system.
- The simplest transposition cipher is made by just writing the message backward.



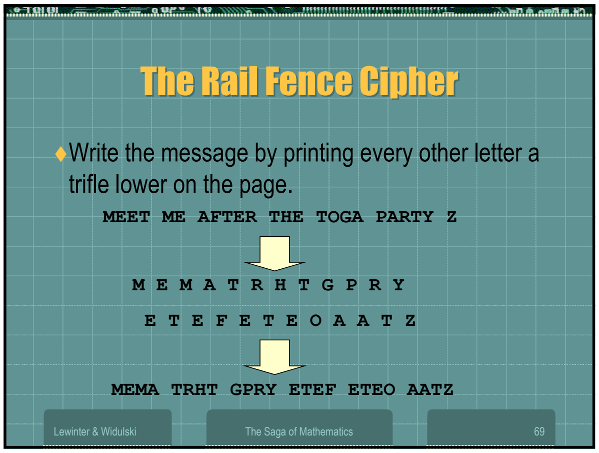
Transposition Ciphers

- Example:
  - THE EAGLE HAS LANDED
- Encoded:
  - DEDNAL SAH ELGAE EHT
- Easy to decode, harder if the original word order is kept, but reverse the letters of each word.
  - EHT ELGAE SAH DEDNAL



The Rail Fence Cipher

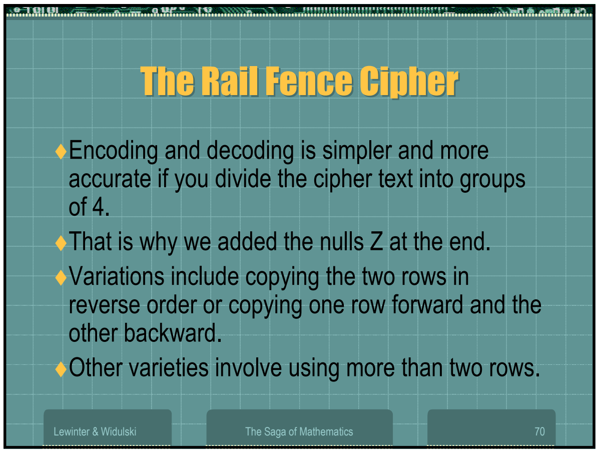
- Count the number of letters.
- If the number is not a multiple of 4, add enough dummy letters (nulls) at the end to make it a multiple of 4.
- Example:
  - **MEET ME AFTER THE TOGA PARTY**
- Add a Z to make it 24 letters long.



The Rail Fence Cipher

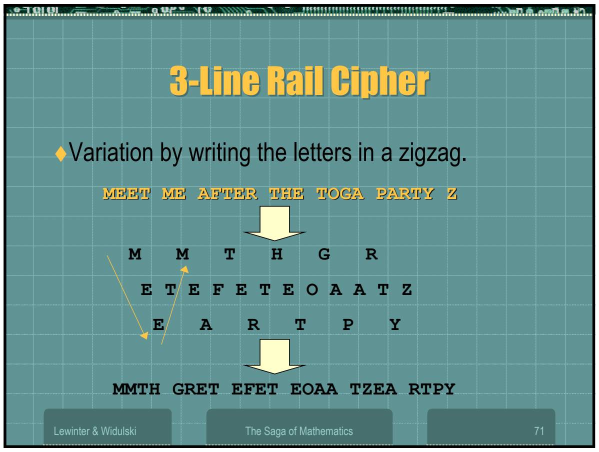
- Write the message by printing every other letter a trifle lower on the page.

```
MEET ME AFTER THE TOGA PARTY Z

   M E M A T R H T G P R Y
    E T E F E T E O A A T Z

MEMA TRHT GPRY ETEF ETEO AATZ
```



The Rail Fence Cipher

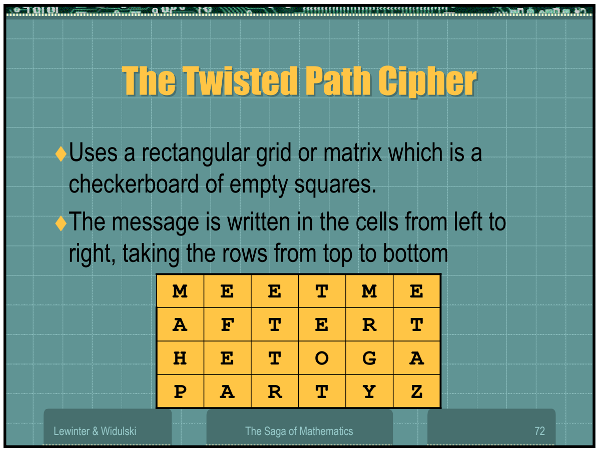
- Encoding and decoding is simpler and more accurate if you divide the cipher text into groups of 4.
- That is why we added the nulls Z at the end.
- Variations include copying the two rows in reverse order or copying one row forward and the other backward.
- Other varieties involve using more than two rows.



3-Line Rail Cipher

- Variation by writing the letters in a zigzag.

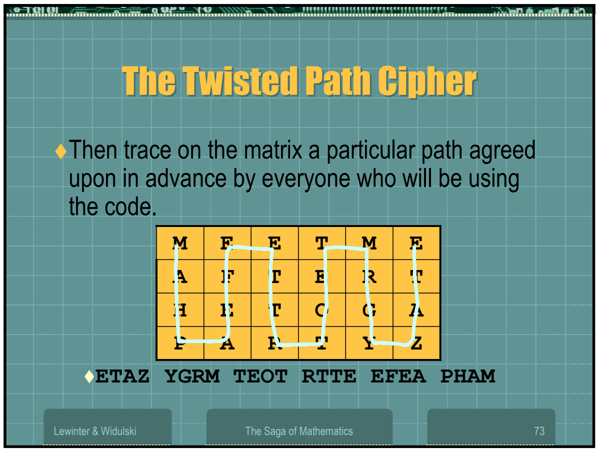
```
MEET ME AFTER THE TOGA PARTY Z

  M   M   T   H   G   R
   E T E F E T E O A A T Z
    E   A   R   T   P   Y

MMTH GRET EFET EOAA TZEA RTPY
```



The Twisted Path Cipher

- Uses a rectangular grid or matrix which is a checkerboard of empty squares.
- The message is written in the cells from left to right, taking the rows from top to bottom

M	E	E	T	M	E
A	F	T	E	R	T
H	E	T	O	G	A
P	A	R	T	Y	Z

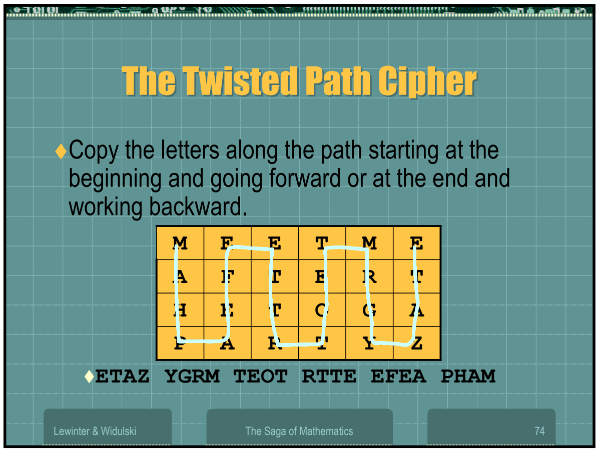


The Twisted Path Cipher

- Then trace on the matrix a particular path agreed upon in advance by everyone who will be using the code.

M	F	E	T	M	E
A	F	T	E	R	T
H	E	T	O	G	A
P	A	R	T	Y	Z

- ETAZ YGRM TEOT RTTE EFEA PHAM

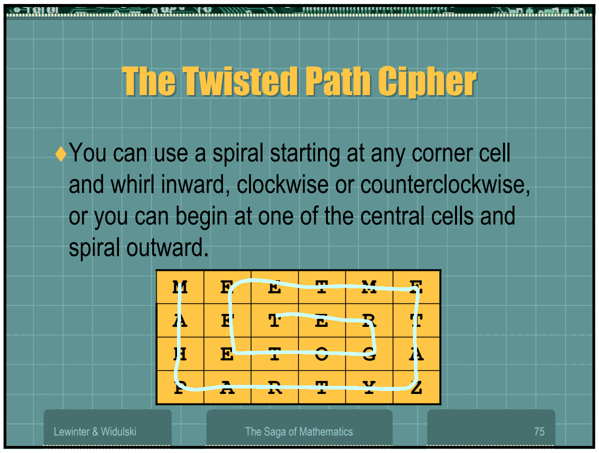


The Twisted Path Cipher

- Copy the letters along the path starting at the beginning and going forward or at the end and working backward.

M	F	E	T	M	E
A	F	T	E	R	T
H	E	T	O	G	A
P	A	R	T	Y	Z

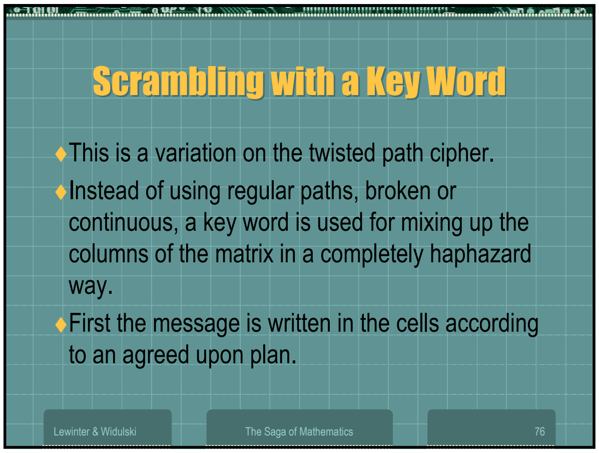
- ETAZ YGRM TEOT RTTE EFEA PHAM



The Twisted Path Cipher

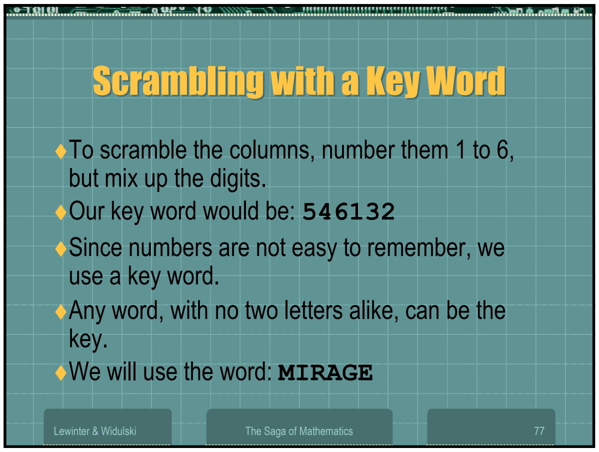
- You can use a spiral starting at any corner cell and whirl inward, clockwise or counterclockwise, or you can begin at one of the central cells and spiral outward.

M	F	E	T	M	E
A	F	T	E	R	T
H	E	T	O	G	A
P	A	R	T	Y	Z



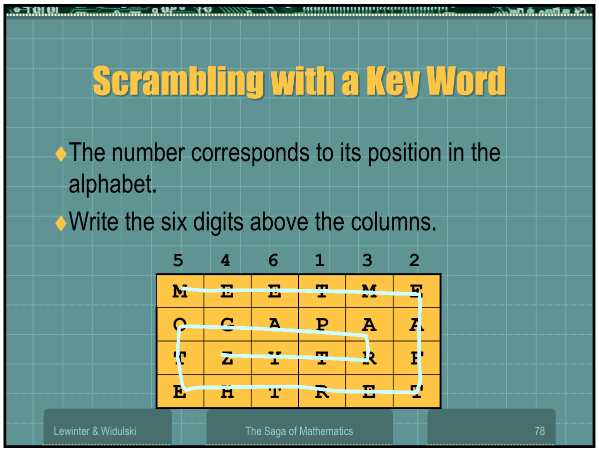
Scrambling with a Key Word

- This is a variation on the twisted path cipher.
- Instead of using regular paths, broken or continuous, a key word is used for mixing up the columns of the matrix in a completely haphazard way.
- First the message is written in the cells according to an agreed upon plan.



Scrambling with a Key Word

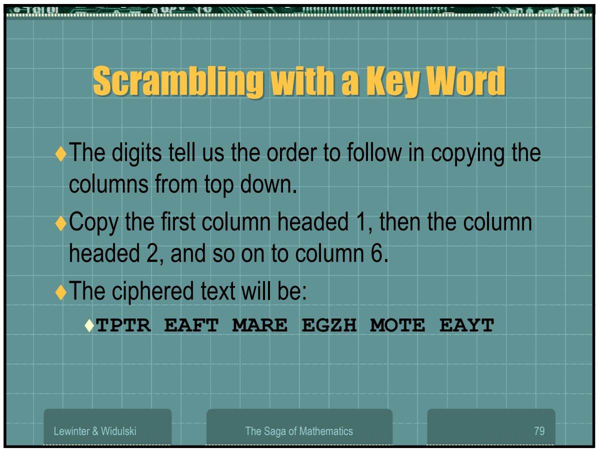
- To scramble the columns, number them 1 to 6, but mix up the digits.
- Our key word would be: **546132**
- Since numbers are not easy to remember, we use a key word.
- Any word, with no two letters alike, can be the key.
- We will use the word: **MIRAGE**



Scrambling with a Key Word

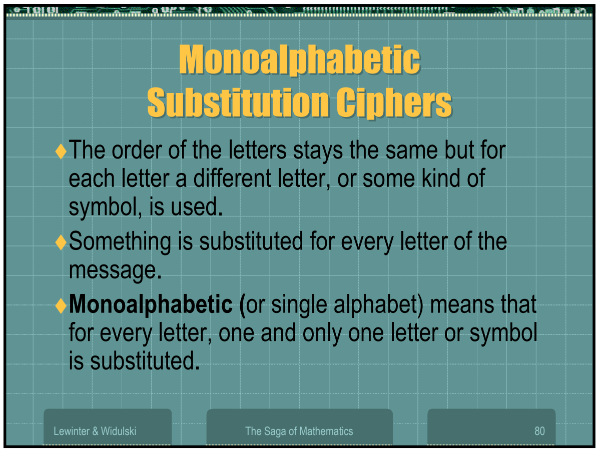
- The number corresponds to its position in the alphabet.
- Write the six digits above the columns.

5	4	6	1	3	2
M	E	E	T	M	E
O	G	A	P	A	A
T	Z	Y	T	R	F
E	H	T	R	E	T



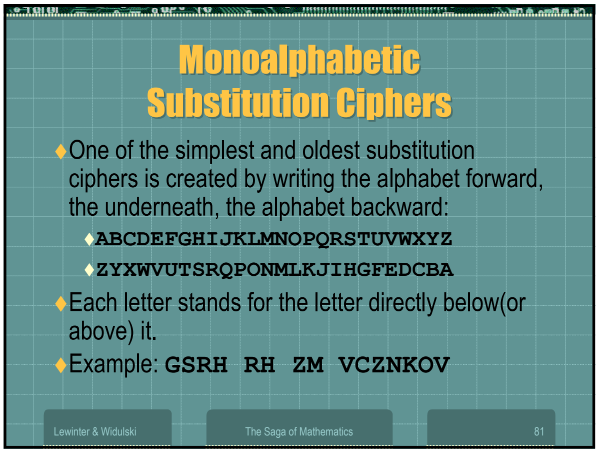
Scrambling with a Key Word

- The digits tell us the order to follow in copying the columns from top down.
- Copy the first column headed 1, then the column headed 2, and so on to column 6.
- The ciphered text will be:
  - **TPTR EAFT MARE EGZH MOTE EAYT**



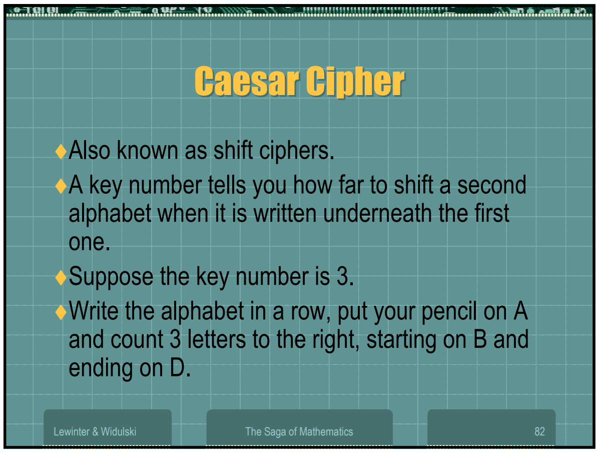
Monoalphabetic Substitution Ciphers

- The order of the letters stays the same but for each letter a different letter, or some kind of symbol, is used.
- Something is substituted for every letter of the message.
- **Monoalphabetic** (or single alphabet) means that for every letter, one and only one letter or symbol is substituted.



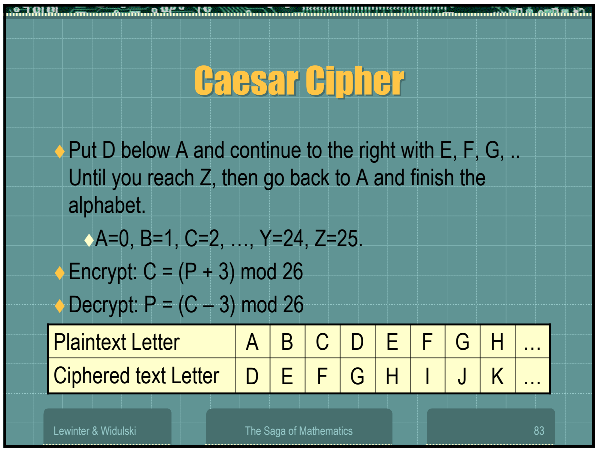
Monoalphabetic Substitution Ciphers

- One of the simplest and oldest substitution ciphers is created by writing the alphabet forward, the underneath, the alphabet backward:
  - **ABCDEFGHIJKLMNOPQRSTUVWXYZ**
  - **ZYXWVUTSRQPONMLKJIHGFEDCBA**
- Each letter stands for the letter directly below(or above) it.
- Example: **GSRH RH ZM VCZNKOV**



Caesar Cipher

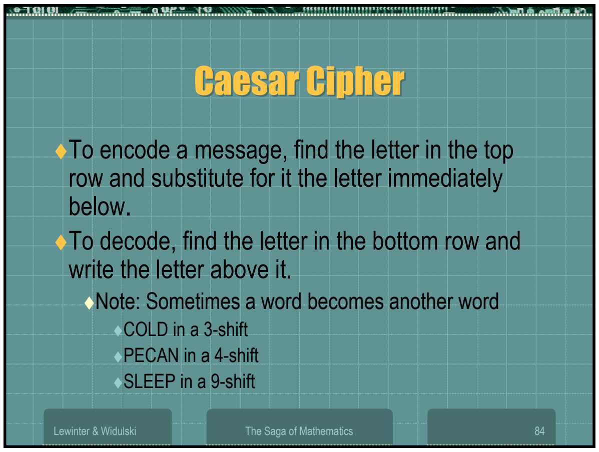
- Also known as shift ciphers.
- A key number tells you how far to shift a second alphabet when it is written underneath the first one.
- Suppose the key number is 3.
- Write the alphabet in a row, put your pencil on A and count 3 letters to the right, starting on B and ending on D.



Caesar Cipher

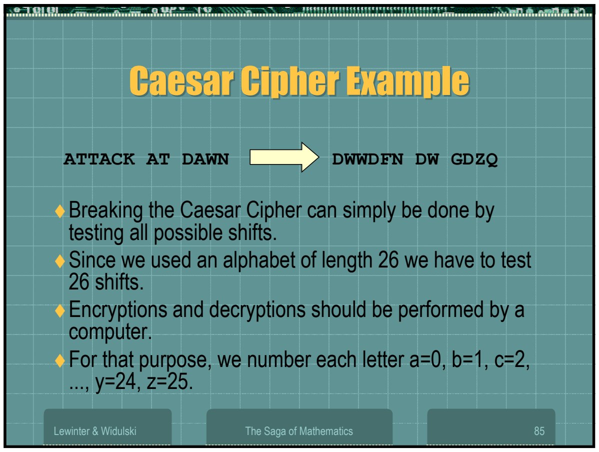
- Put D below A and continue to the right with E, F, G, .. Until you reach Z, then go back to A and finish the alphabet.
  - A=0, B=1, C=2, …, Y=24, Z=25.
- Encrypt: C = (P + 3) mod 26
- Decrypt: P = (C – 3) mod 26

Plaintext Letter	A	B	C	D	E	F	G	H	…
Ciphered text Letter	D	E	F	G	H	I	J	K	…



Caesar Cipher

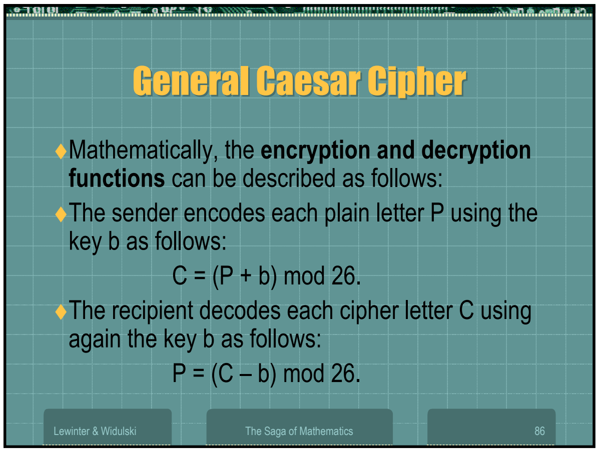
- To encode a message, find the letter in the top row and substitute for it the letter immediately below.
- To decode, find the letter in the bottom row and write the letter above it.
  - Note: Sometimes a word becomes another word
    - COLD in a 3-shift
    - PECAN in a 4-shift
    - SLEEP in a 9-shift



Caesar Cipher Example

`ATTACK AT DAWN` → `DWWDFN DW GDZQ`

- Breaking the Caesar Cipher can simply be done by testing all possible shifts.
- Since we used an alphabet of length 26 we have to test 26 shifts.
- Encryptions and decryptions should be performed by a computer.
- For that purpose, we number each letter a=0, b=1, c=2, ..., y=24, z=25.

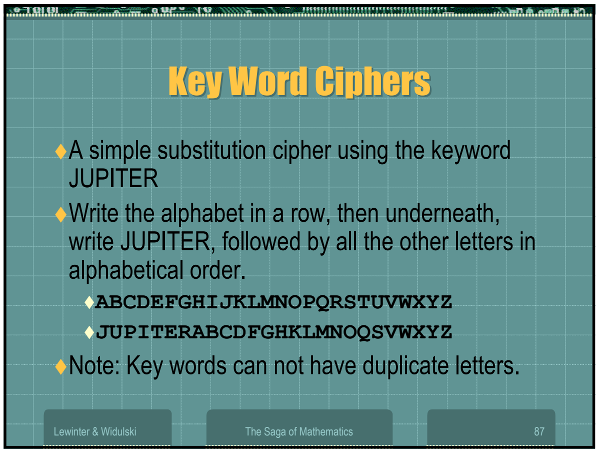


General Caesar Cipher

- Mathematically, the **encryption and decryption functions** can be described as follows:
- The sender encodes each plain letter P using the key b as follows:

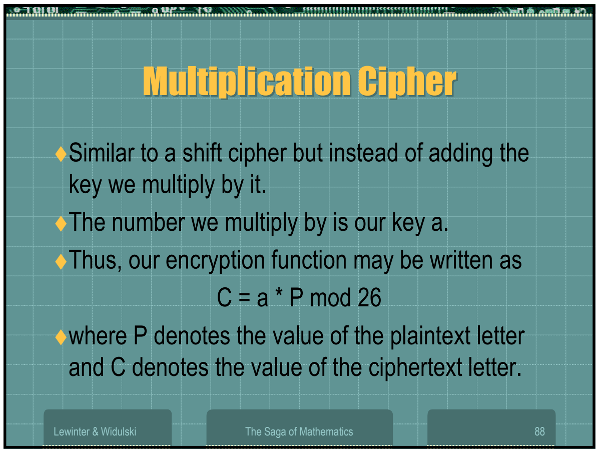
  C = (P + b) mod 26.
- The recipient decodes each cipher letter C using again the key b as follows:

  P = (C – b) mod 26.



Key Word Ciphers

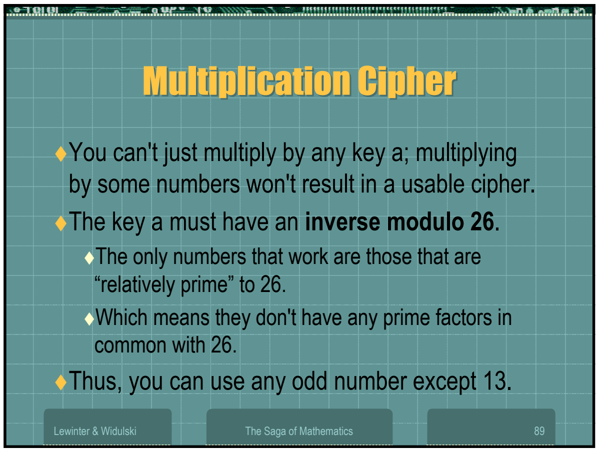
- A simple substitution cipher using the keyword JUPITER
- Write the alphabet in a row, then underneath, write JUPITER, followed by all the other letters in alphabetical order.
  - **ABCDEFGHIJKLMNOPQRSTUVWXYZ**
  - **JUPITERABCDFGHKLMNOQSVWXYZ**
- Note: Key words can not have duplicate letters.



Multiplication Cipher

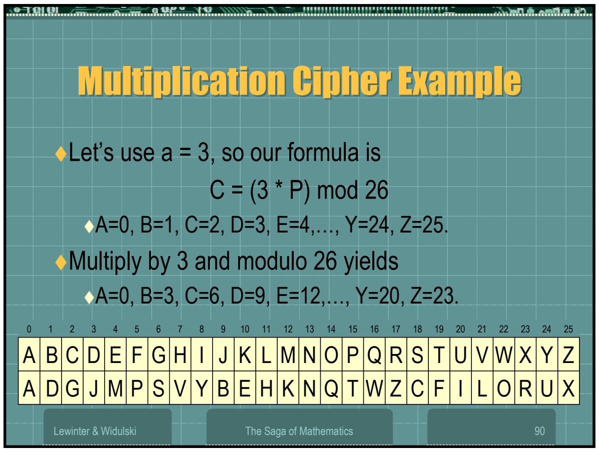
- Similar to a shift cipher but instead of adding the key we multiply by it.
- The number we multiply by is our key a.
- Thus, our encryption function may be written as

  C = a * P mod 26
- where P denotes the value of the plaintext letter and C denotes the value of the ciphertext letter.



Multiplication Cipher

- You can't just multiply by any key a; multiplying by some numbers won't result in a usable cipher.
- The key a must have an **inverse modulo 26**.
  - The only numbers that work are those that are “relatively prime” to 26.
  - Which means they don't have any prime factors in common with 26.
- Thus, you can use any odd number except 13.

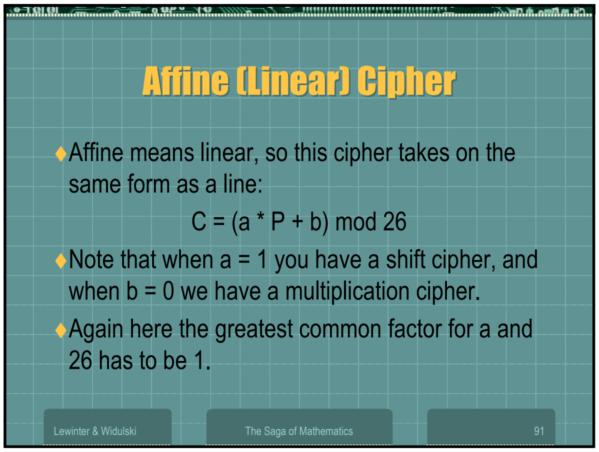


Multiplication Cipher Example

- Let’s use a = 3, so our formula is

  C = (3 * P) mod 26
  - A=0, B=1, C=2, D=3, E=4,…, Y=24, Z=25.
- Multiply by 3 and modulo 26 yields
  - A=0, B=3, C=6, D=9, E=12,…, Y=20, Z=23.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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
A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X

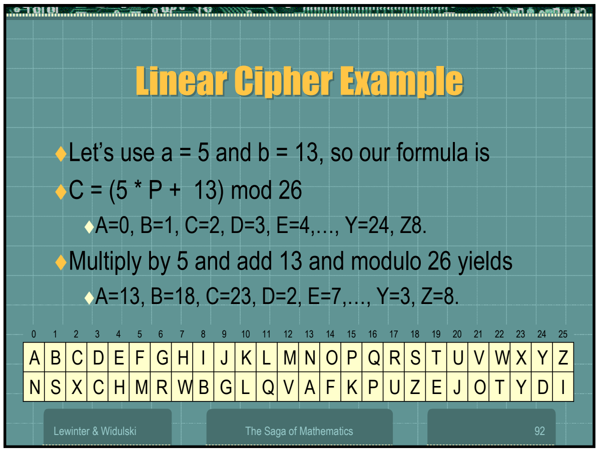


Affine (Linear) Cipher

- Affine means linear, so this cipher takes on the same form as a line:

  C = (a * P + b) mod 26

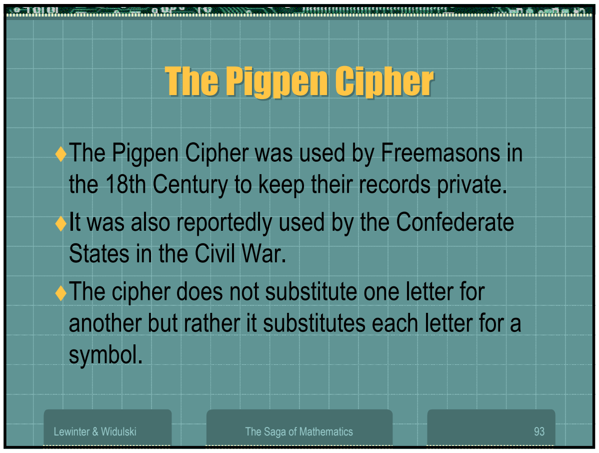
- Note that when a = 1 you have a shift cipher, and when b = 0 we have a multiplication cipher.
- Again here the greatest common factor for a and 26 has to be 1.



Linear Cipher Example

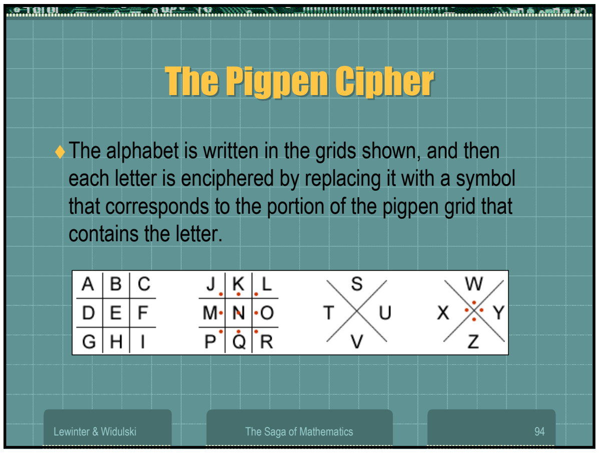
- Let's use a = 5 and b = 13, so our formula is
- C = (5 * P + 13) mod 26
  - A=0, B=1, C=2, D=3, E=4,…, Y=24, Z8.
- Multiply by 5 and add 13 and modulo 26 yields
  - A=13, B=18, C=23, D=2, E=7,…, Y=3, Z=8.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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
N	S	X	C	H	M	R	W	B	G	L	Q	V	A	F	K	P	U	Z	E	J	O	T	Y	D	I



The Pigpen Cipher

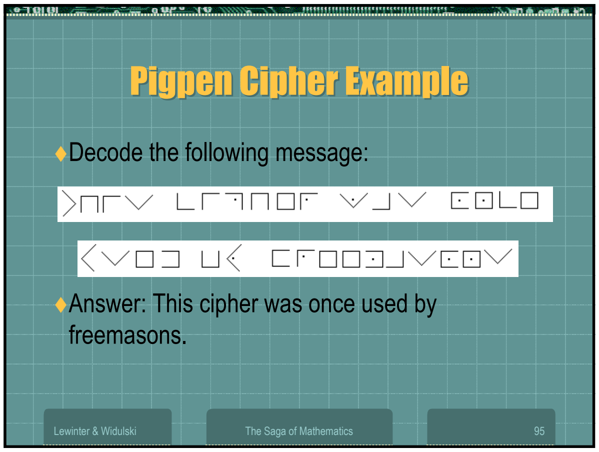
- The Pigpen Cipher was used by Freemasons in the 18th Century to keep their records private.
- It was also reportedly used by the Confederate States in the Civil War.
- The cipher does not substitute one letter for another but rather it substitutes each letter for a symbol.



The Pigpen Cipher

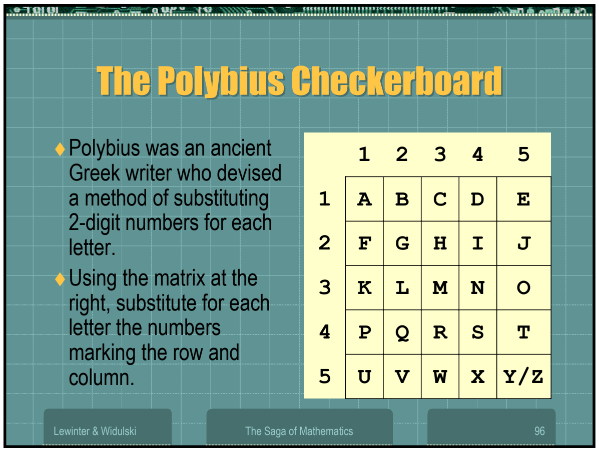
- The alphabet is written in the grids shown, and then each letter is enciphered by replacing it with a symbol that corresponds to the portion of the pigpen grid that contains the letter.

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



Pigpen Cipher Example

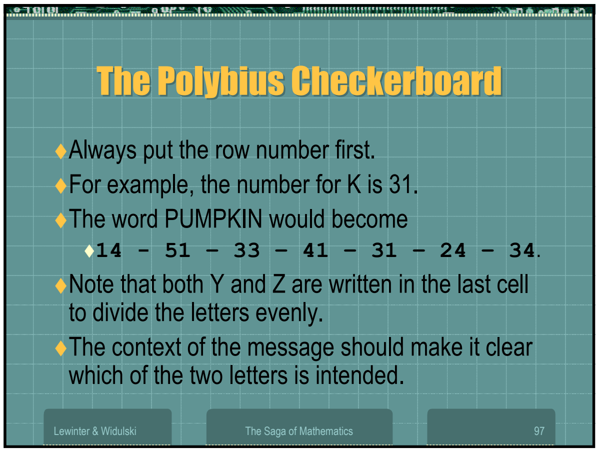
- Decode the following message:
- Answer: This cipher was once used by freemasons.



The Polybius Checkerboard

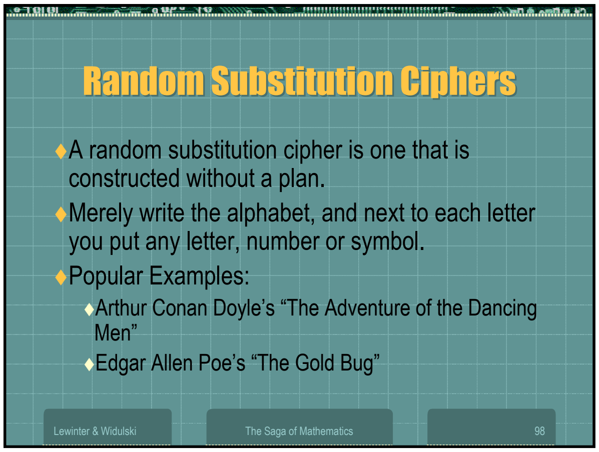
- Polybius was an ancient Greek writer who devised a method of substituting 2-digit numbers for each letter.
- Using the matrix at the right, substitute for each letter the numbers marking the row and column.

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



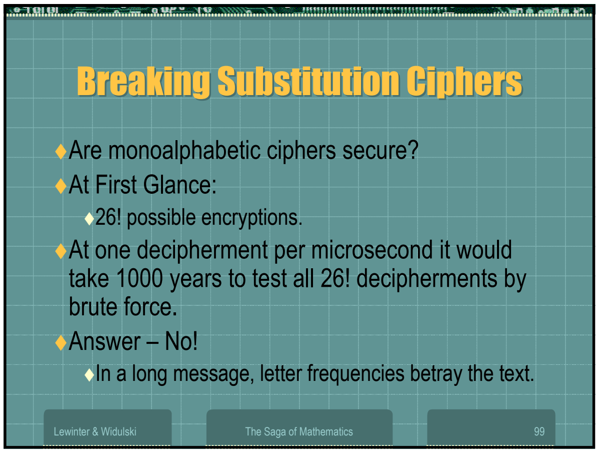
The Polybius Checkerboard

- Always put the row number first.
- For example, the number for K is 31.
- The word PUMPKIN would become
  - **14 – 51 – 33 – 41 – 31 – 24 – 34**.
- Note that both Y and Z are written in the last cell to divide the letters evenly.
- The context of the message should make it clear which of the two letters is intended.



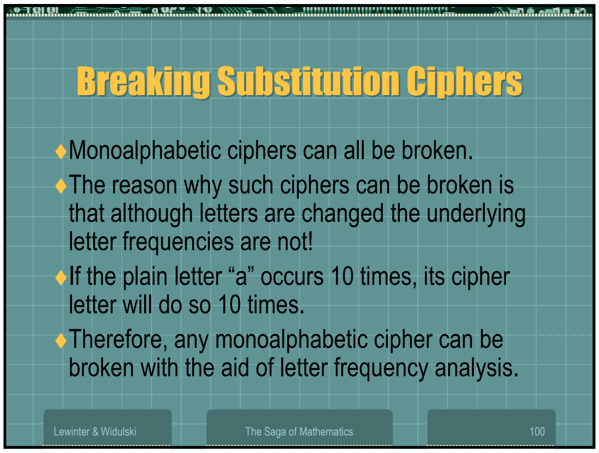
Random Substitution Ciphers

- A random substitution cipher is one that is constructed without a plan.
- Merely write the alphabet, and next to each letter you put any letter, number or symbol.
- Popular Examples:
  - Arthur Conan Doyle's "The Adventure of the Dancing Men"
  - Edgar Allen Poe's "The Gold Bug"



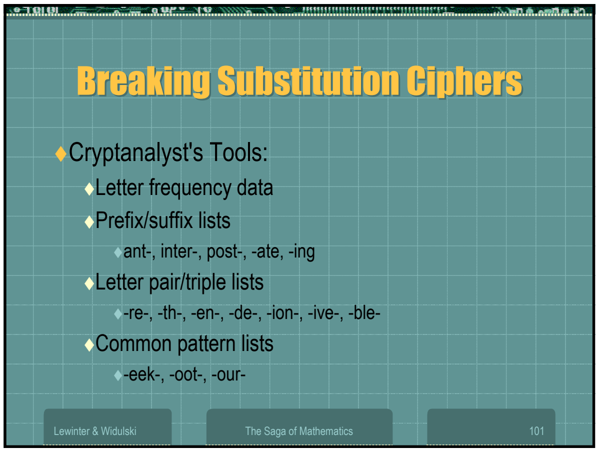
Breaking Substitution Ciphers

- Are monoalphabetic ciphers secure?
- At First Glance:
  - 26! possible encryptions.
- At one decipherment per microsecond it would take 1000 years to test all 26! decipherments by brute force.
- Answer – No!
  - In a long message, letter frequencies betray the text.



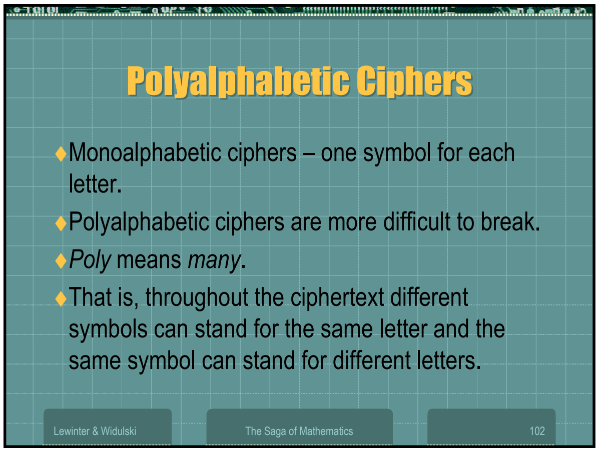
Breaking Substitution Ciphers

- Monoalphabetic ciphers can all be broken.
- The reason why such ciphers can be broken is that although letters are changed the underlying letter frequencies are not!
- If the plain letter "a" occurs 10 times, its cipher letter will do so 10 times.
- Therefore, any monoalphabetic cipher can be broken with the aid of letter frequency analysis.



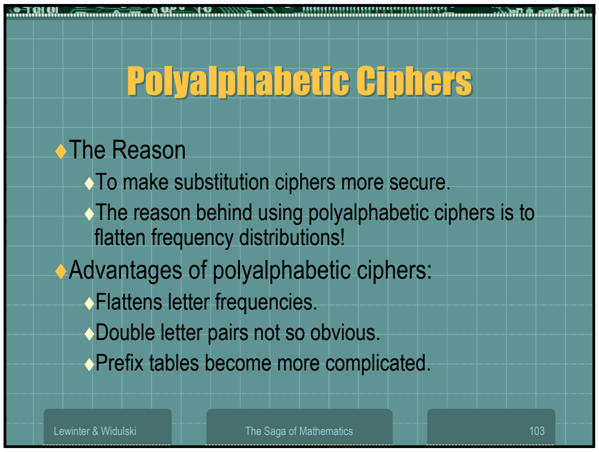
Breaking Substitution Ciphers

- Cryptanalyst's Tools:
  - Letter frequency data
  - Prefix/suffix lists
    - ant-, inter-, post-, -ate, -ing
  - Letter pair/triple lists
    - -re-, -th-, -en-, -de-, -ion-, -ive-, -ble-
  - Common pattern lists
    - -eek-, -oot-, -our-



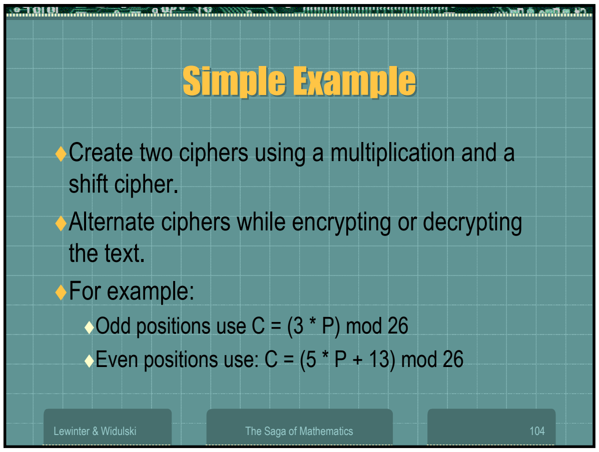
Polyalphabetic Ciphers

- Monoalphabetic ciphers – one symbol for each letter.
- Polyalphabetic ciphers are more difficult to break.
- *Poly* means *many*.
- That is, throughout the ciphertext different symbols can stand for the same letter and the same symbol can stand for different letters.



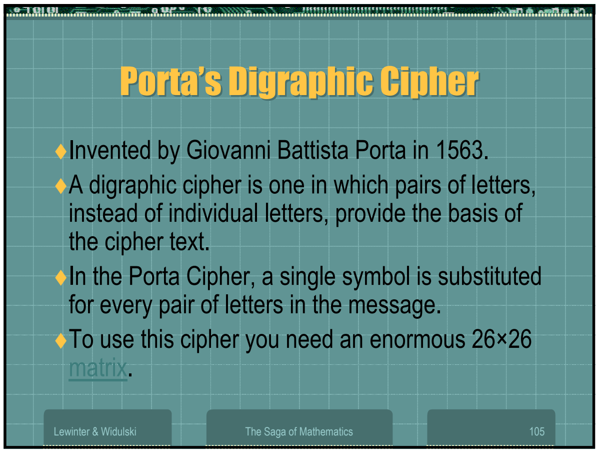
Polyalphabetic Ciphers

- The Reason
  - To make substitution ciphers more secure.
  - The reason behind using polyalphabetic ciphers is to flatten frequency distributions!
- Advantages of polyalphabetic ciphers:
  - Flattens letter frequencies.
  - Double letter pairs not so obvious.
  - Prefix tables become more complicated.



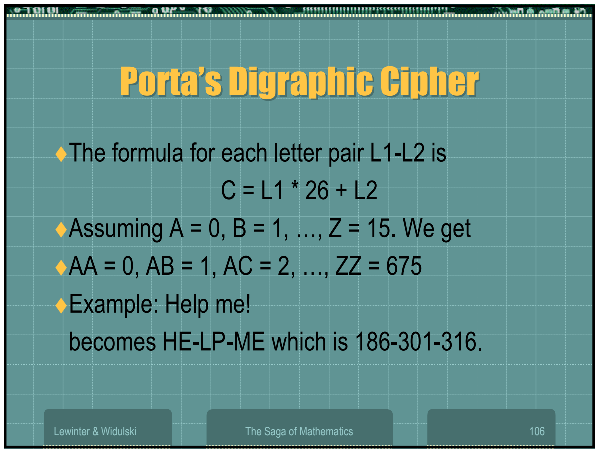
Simple Example

- Create two ciphers using a multiplication and a shift cipher.
- Alternate ciphers while encrypting or decrypting the text.
- For example:
  - Odd positions use C = (3 * P) mod 26
  - Even positions use: C = (5 * P + 13) mod 26



Porta's Digraphic Cipher

- Invented by Giovanni Battista Porta in 1563.
- A digraphic cipher is one in which pairs of letters, instead of individual letters, provide the basis of the cipher text.
- In the Porta Cipher, a single symbol is substituted for every pair of letters in the message.
- To use this cipher you need an enormous 26×26 matrix.

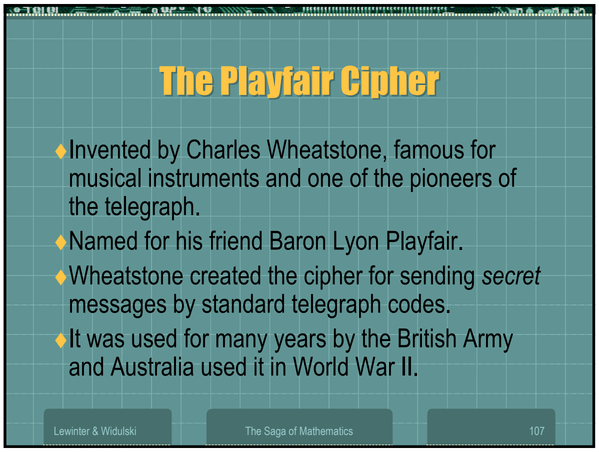


Porta's Digraphic Cipher

- The formula for each letter pair L1-L2 is

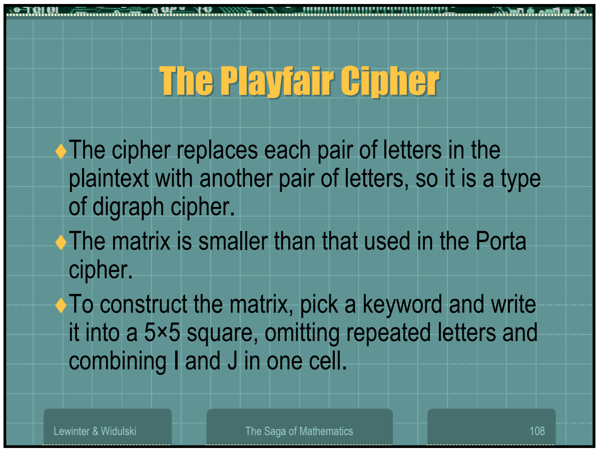
  C = L1 * 26 + L2
- Assuming A = 0, B = 1, …, Z = 15. We get
- AA = 0, AB = 1, AC = 2, …, ZZ = 675
- Example: Help me!

  becomes HE-LP-ME which is 186-301-316.



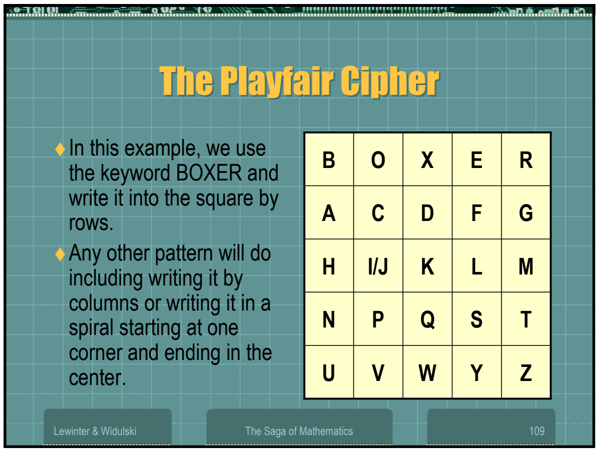
The Playfair Cipher

- Invented by Charles Wheatstone, famous for musical instruments and one of the pioneers of the telegraph.
- Named for his friend Baron Lyon Playfair.
- Wheatstone created the cipher for sending *secret* messages by standard telegraph codes.
- It was used for many years by the British Army and Australia used it in World War II.



The Playfair Cipher

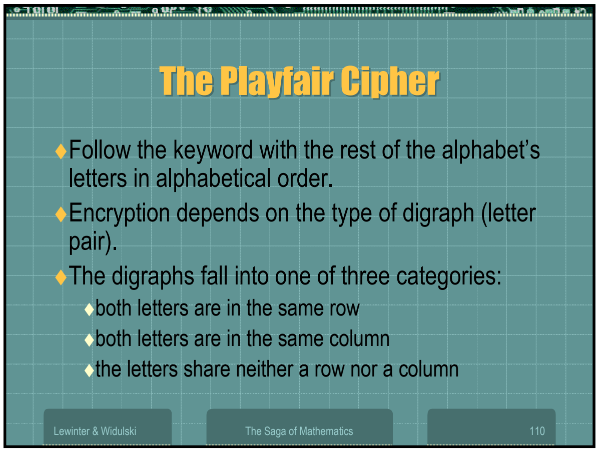
- The cipher replaces each pair of letters in the plaintext with another pair of letters, so it is a type of digraph cipher.
- The matrix is smaller than that used in the Porta cipher.
- To construct the matrix, pick a keyword and write it into a 5×5 square, omitting repeated letters and combining I and J in one cell.



The Playfair Cipher

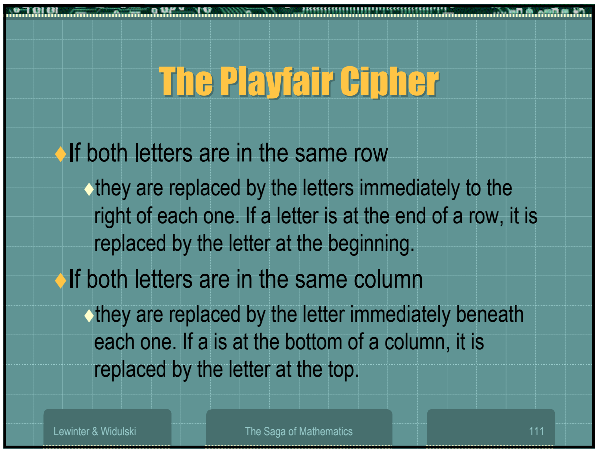
- In this example, we use the keyword BOXER and write it into the square by rows.
- Any other pattern will do including writing it by columns or writing it in a spiral starting at one corner and ending in the center.

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



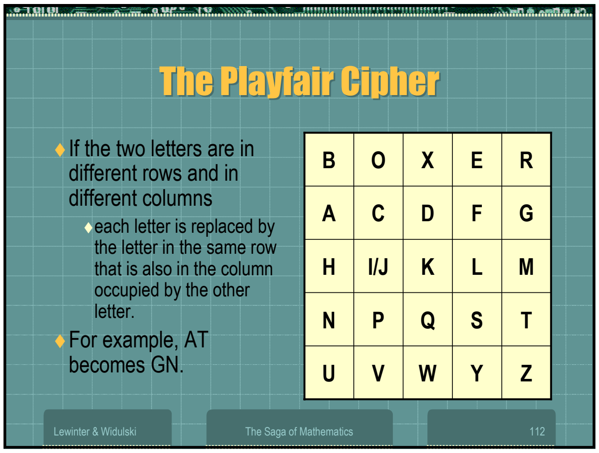
The Playfair Cipher

- Follow the keyword with the rest of the alphabet's letters in alphabetical order.
- Encryption depends on the type of digraph (letter pair).
- The digraphs fall into one of three categories:
  - both letters are in the same row
  - both letters are in the same column
  - the letters share neither a row nor a column



The Playfair Cipher

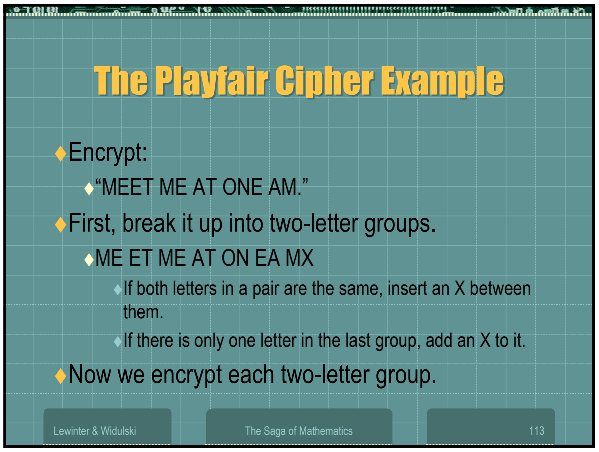
- If both letters are in the same row
  - they are replaced by the letters immediately to the right of each one. If a letter is at the end of a row, it is replaced by the letter at the beginning.
- If both letters are in the same column
  - they are replaced by the letter immediately beneath each one. If a is at the bottom of a column, it is replaced by the letter at the top.



The Playfair Cipher

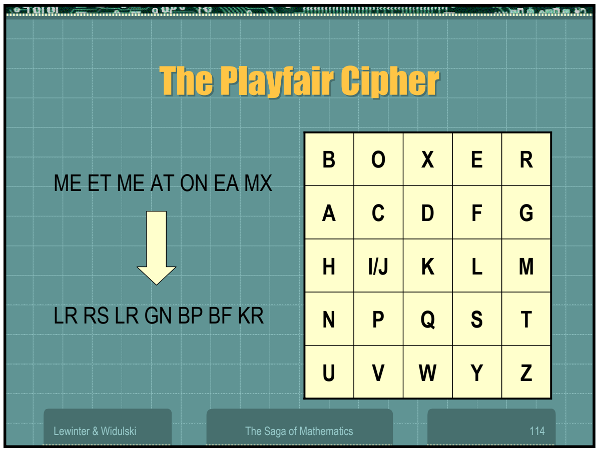
- If the two letters are in different rows and in different columns
  - each letter is replaced by the letter in the same row that is also in the column occupied by the other letter.
- For example, AT becomes GN.

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



The Playfair Cipher Example

- Encrypt:
  - "MEET ME AT ONE AM."
- First, break it up into two-letter groups.
  - ME ET ME AT ON EA MX
    - If both letters in a pair are the same, insert an X between them.
    - If there is only one letter in the last group, add an X to it.
- Now we encrypt each two-letter group.



The Playfair Cipher

ME ET ME AT ON EA MX

LR RS LR GN BP BF KR

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

The Playfair Cipher

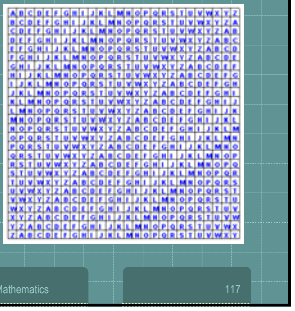
- To decrypt the message, simply reverse the process:
  - If the two letters are in different rows and columns, take the letters in the opposite corners of their rectangle.
  - If they are in the same row, take the letters to the left.
  - If they are in the same column, take the letters above each of them.

The Vigenere Cipher

- Named for Blaise de Vigenere a 16th century Frenchman.
- The **Vigenere cipher** is a polyalphabetic cipher based on using successively shifted alphabets, a different shifted alphabet for each of the 26 English letters.
- The procedure is based on the table shown on the next slide and the use of a keyword.

The Vigenere Cipher

- Note that each row of the matrix corresponds to a Caesar Cipher.
  - The first row is a shift of 0
  - the second is a shift of 1 and
  - the last is a shift of 25.
- For a better matrix click here.



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

The Vigenere Cipher

One Method of Using the Vigenere Table:

1. Choose a key.
2. Break text into groups of five characters.
3. Write the key in repeating fashion.
4. Use letter of key to establish column.
5. Use plaintext to establish row.
6. Encrypt by using intersection of row and column.

The Vigenere Cipher Example

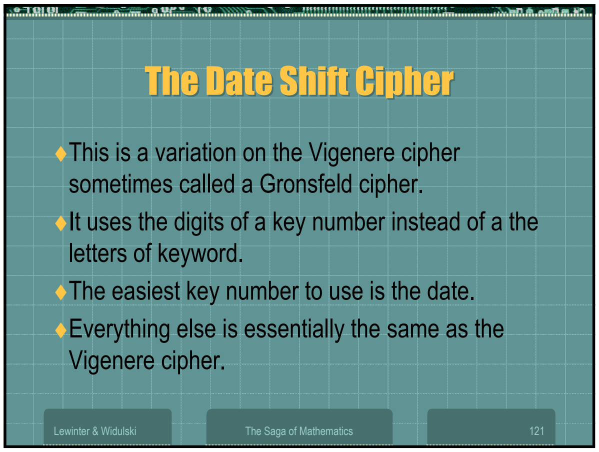
- The keyword is **CIPHER**.
- The message is **MEET ME AT ONE AM**.

```
C I P H E R C I P H E R C
M E E T M E A T O N E A M
-------------------------
O M T A Q V C B D U I R O
```

- Encrypted becomes **OMTA QVCB DDUI RO**.

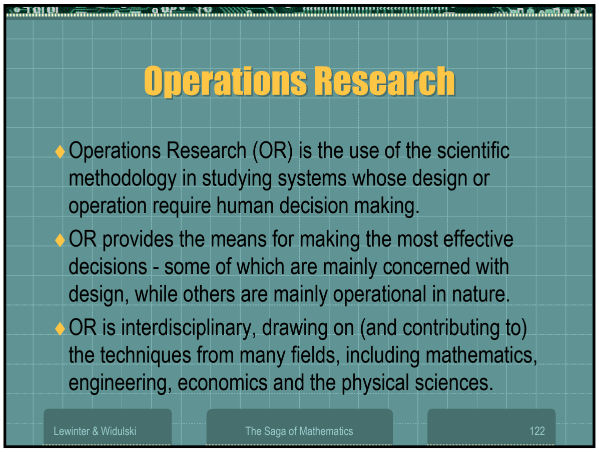
The Vigenere Cipher

- A computer program would implement the following algorithm:
  - Code the letters as numbers (A=0, B=1, etc.)
  - The key is keyword
  - To Encrypt: Add the keyword to the plaintext (letter by letter)
  - To Decrypt: Subtract keyword from the ciphertext



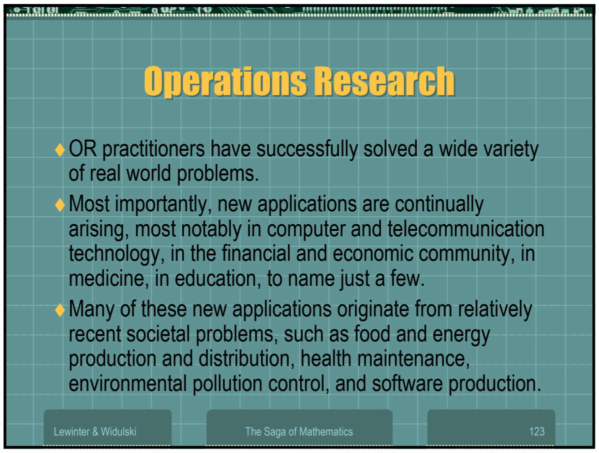
The Date Shift Cipher

- This is a variation on the Vigenere cipher sometimes called a Gronsfeld cipher.
- It uses the digits of a key number instead of a the letters of keyword.
- The easiest key number to use is the date.
- Everything else is essentially the same as the Vigenere cipher.



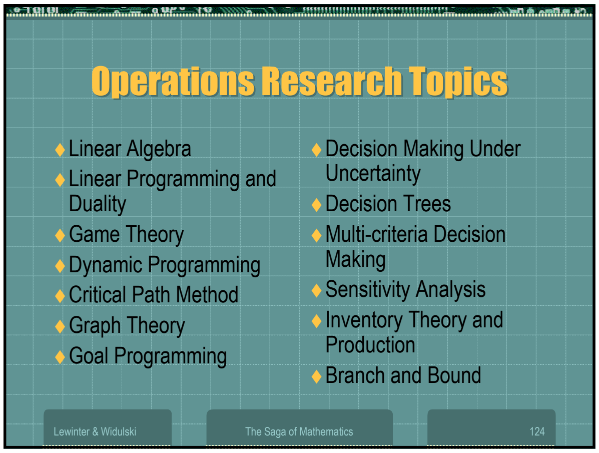
Operations Research

- Operations Research (OR) is the use of the scientific methodology in studying systems whose design or operation require human decision making.
- OR provides the means for making the most effective decisions - some of which are mainly concerned with design, while others are mainly operational in nature.
- OR is interdisciplinary, drawing on (and contributing to) the techniques from many fields, including mathematics, engineering, economics and the physical sciences.



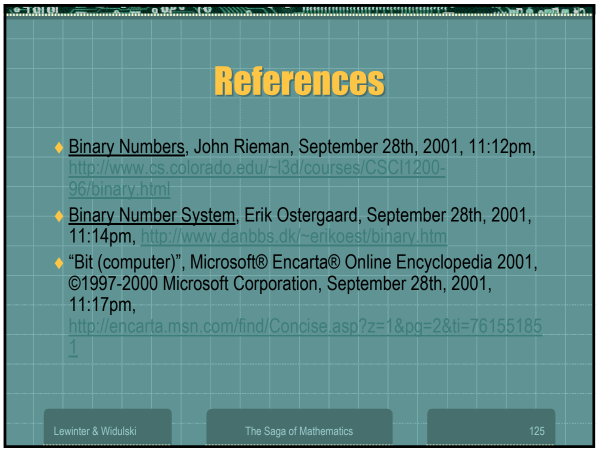
Operations Research

- OR practitioners have successfully solved a wide variety of real world problems.
- Most importantly, new applications are continually arising, most notably in computer and telecommunication technology, in the financial and economic community, in medicine, in education, to name just a few.
- Many of these new applications originate from relatively recent societal problems, such as food and energy production and distribution, health maintenance, environmental pollution control, and software production.



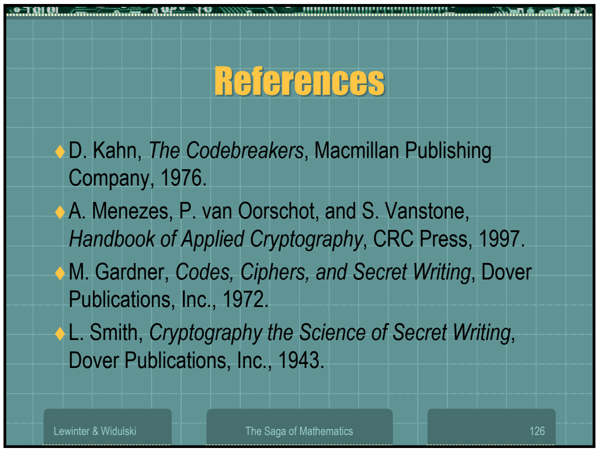
Operations Research Topics

- Linear Algebra
- Linear Programming and Duality
- Game Theory
- Dynamic Programming
- Critical Path Method
- Graph Theory
- Goal Programming
- Decision Making Under Uncertainty
- Decision Trees
- Multi-criteria Decision Making
- Sensitivity Analysis
- Inventory Theory and Production
- Branch and Bound



References

- Binary Numbers, John Rieman, September 28th, 2001, 11:12pm, http://www.cs.colorado.edu/~l3d/courses/CSCI1200-96/binary.html
- Binary Number System, Erik Ostergaard, September 28th, 2001, 11:14pm, http://www.danbbs.dk/~erikoest/binary.htm
- “Bit (computer)”, Microsoft® Encarta® Online Encyclopedia 2001, ©1997-2000 Microsoft Corporation, September 28th, 2001, 11:17pm, http://encarta.msn.com/find/Concise.asp?z=1&pg=2&ti=761551851



References

- D. Kahn, *The Codebreakers*, Macmillan Publishing Company, 1976.
- A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
- M. Gardner, *Codes, Ciphers, and Secret Writing*, Dover Publications, Inc., 1972.
- L. Smith, *Cryptography the Science of Secret Writing*, Dover Publications, Inc., 1943.

Web Sites

- Check out Computer History web site.
- The Black Chamber web site.
- The GCHQ web site.
- The Crypto Tutorial web site.
- A Cryptographic Compendium
- The SSH website
- Check out Operations Research Tutor web site.