# Computer Security

A [Not So?] Short History of Cryptography





# Sources

- Two absolutely fascinating books:
  - ***The Codebreakers***, David Kahn, 1996, Scribner
  - ***The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography***, by Simon Singh, 1999, Anchor Books

  Both highly recommended; both very readable.

- Various web sites



# Ancient Egypt

- Tomb of Khnumhotep II
  - Inscriptions recording the monuments Khnumhotep had erected in the service of pharaoh Amenemhet
  - The scribe used hieroglyphic substitutions to impart dignity and authority
  - Not really secret writing, but uses a deliberate transformation of the writing.
  - The oldest text known to do so.



# Ancient China

- Used a technique of hiding messages:
  - Write a message on a piece of very thin silk or paper
  - Roll it up into a ball, and cover it with wax to produce a wax ball ("la wan")
  - Messenger would hide the wax ball on his person, or in his rectum, or swallow it.

# Ancient India

- Vatsyanyana's famous textbook of erotics, the *Kama-sutra*:
  - Lists 64 arts, or *yogas*, that women should know and practice, from vocal music through prestidigitation*
  - 45th in the list is secret writing, (*mlecchita-vikalpa*) advocated "in order to help women conceal the details of their liaisons"
  - Two forms:
    - *Kautiliyam* : uses letter subsitutions based on phonetic relations
    - *Muladeviya* : uses a cipher alphabet

***pres·ti·dig·i·ta·tion**
**:** Sleight of hand, legerdemain



# Ancient Mesopotamia

- The oldest Mesopotamian encipherment:
  - A 3" x 2" cuneiform* tablet, dating from ~1500 B.C.
  - Earliest known formula for pottery glazes.
  - Uses cuneiform signs in their least common syllabic values to attempt to hide the secrets of the formulae
  - "Like George Bernard Shaw's rewriting of *fish* as *ghoti*"

***cu·ne·i·form**
**1** : having the shape of a wedge
**2** : composed of or written in wedge-shaped characters
<*cuneiform* syllabary>



# Babylonia and Assyria

- Scribes sometimes used rare or unusual cuneiform signs in signing and dating their clay tablets.
  - Ending formulas, known as *colophons**
  - Short and stereotyped
  - Substitutions intended to impress later readers of the scribe's knowledge.

***col·o·phon**
**1** : an inscription placed at the end of a book or manuscript usually with facts relative to its production
**2** : an identifying device used by a printer or a publisher

**(For a modern-day colophon, see the back of virtually any O'Reilly & Associates book.)**



# Hebrew Tradition

- Lists three different transformations in the Old Testament.
  - Jeremiah 25:26 and 51:41
  - Jeremiah 51:1
  - Isaiah 7:6
- Probably motivations of pride and wish for immortality, as later scholars would copy and transmit to posterity.

# Ancient Greece

- Polybius (c.200 - 118 B.C.)
  - The noted Greek philosopher, historian and writer Polybius arranged the alphabet into a squared grid or matrix. By numbering the rows and columns, letters could be transformed into other paired characters.
  - The Polybius square's features of splitting a character into two parts, reducing the number of characters needed and ability to convert letters into numbers is still used in modern algorithms.

| | 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 |



# Ancient Greece

- Heroditus, in *The Histories*, chronicled the conflicts between Greece and Persia in the 5th century B.C.
  - Xerxes, king of Persia, was assembling a fighting force, and planned a surprise attack on the Greeks
  - Demaratus, an expelled Greek who lived in Persia, sent a secret message to the Greeks -- writing on wooden folding tablets, and covered with wax
  - Greece, having been warned, turned the tables, surprised the Persian fleet, and defeated it.



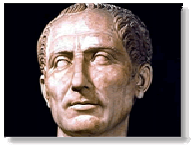
# Ancient Greece

- The Spartan *scytale* (or *skytale*) dates back to the fifth century B.C.
  - The scytale is a wooden staff around which a strip of leather or parchment is wound.
  - The sender writes the message along the length of the scytale, and then unwinds the strip, perhaps disguising it as a belt.
  - The message recipient simply rewinds the strip around his scytale and reads the message.
  - Lysander of Sparta was the recipient of such a message, which warned him that Pharnabazus of Persia was about to attack. Thus warned, he repulsed the attack.



# Ancient Greece

- The Ancient Greeks produced the first instructional text on communication security:
  - An entire chapter in one of the earliest works on military science, *On the Defense of Fortified Places*, by Aeneas the Tactician.
  - Described various techniques for enciphering messages



# Ancient Rome

- The first documented use of a substitution cipher for military purposes appears in Julius Caesar's *Gallic Wars*
- Caesar sent a message to Cicero, who was besieged and on the verge of surrender.
- The substitution replaced Roman letters with Greek letters, rendering the message unintelligible to the enemy.
- Another type of cipher used by Caesar simply replaced each letter in the message with the letter that is three places further down the alphabet, looping back to the beginning of the alphabet when there are no more letters available.

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |



# Scandinavia and Anglo-Saxon Britain

- *Runes** flourished in Scandinavia and in Anglo-Saxon Britain during the 7th, 8th and 9th centuries and were occasionally enciphered.
- Runes were almost always used for religious purposes

***rune**
**1 :** any of the characters of any of several alphabets used by the Germanic peoples from about the 3rd to the 13th centuries
**2 :** mystery, magic
**3** [Finnish *runo*, of Germanic origin; akin to Old Norse *run*] **a :** a Finnish or Old Norse poem **b :** poem, song



# Celtic Britain

- *Ogham** survives principally in inscriptions on tombstones.
  - Methods for enciphering them are cataloged in the *Book of Ballymote*, a 15th century compilation of historical, genealogical, and other important facts.
  - The names of these enciphering methods are delightful:
    - "The ogham that bewildered Bres"
    - "Serpent through the heather"
    - "Great speckle"
    - "Vexation of a poet's heart", etc.

***ogham**
: the alphabetic system of 5th and 6th century Irish in which an alphabet of 20 letters is represented by notches for vowels and lines for consonants and which is known principally from inscriptions cut on the edges of rough standing tombstones



# The Middle Ages

- Roger Bacon, an English monk, wrote an *Epistle on the Secret Works of Art and the Nullity of Magic* in the 13th century.
  - Describes seven deliberately vague methods of concealing a secret.
- In the 14th century, Geoffrey Chaucer, most famous for his *Canterbury Tales*, was an English customs official, amateur astronomer, and literary genius
  - In his *Treatise on the Astrolabe**, which describes the workings of an astronomical instrument, he provided additional notes, *The Equatorie of the Planetis*, in which he included six short passages in cipher

***as·tro·labe**
: a compact instrument used to observe and calculate the position of celestial bodies before the invention of the sextant

# Arabia

- Cryptology was born among the Arabs, starting around 855 A.D.
- 8th cent. - Abu 'Abd al-Rahman al-Khalil ibn Ahmad ibn 'Amr ibn Tammam al Farahidi al-Zadi al Yahmadi (how about that for a name?) finds the solution for a Greek cryptogram by first of all finding out the plaintext behind the encryption, a method which never became outdated
- The first to discover and write down the methods of cryptanalysis.
- Extremist sects in Islam cultivated cryptography to conceal their writings from the orthodox.
- In 1412, the Arabic knowledge of cryptography was fully set forth in the section on cryptology in the *Subh al-a 'sha*, a huge 14-volume encyclopedia



# Europe and the Renaissance

- After the Middle Ages, the importance of cryptography and cryptanalysis increased, with many powerful city states employing them to their advantage
  - Venice, Florence
  - Henry II of France
  - In particular, the Vatican became very involved in cryptography, and appears to have influenced many of the major inventions in the subject.
- Cryptography was even mentioned in *The Art of War*, by Machiavelli.



# Mary Queen of Scots

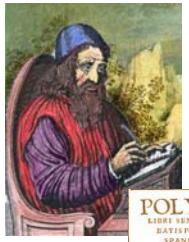
- Mary Queen of Scots used a cipher to communicate with fellow Catholic conspirators in an attempt to overthrow her cousin, the Protestant Queen Elizabeth I of England
- Sir Francis Walsingham, Elizabeth's Principal Secretary and "England's spymaster" intercepted the messages.
- Thomas Phelippes, England's first great cryptanalyst, whose master was Walsingham, deciphered the messages. He also forged a postscript to one of the messages in order to learn the identities of six conspirators
- The evidence of the deciphered messages gave rise to Mary's conviction, and her eventual beheading in 1587.

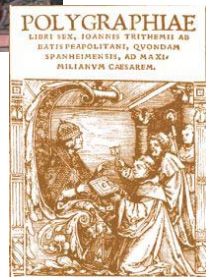


# The Beginnings of Modern Cryptography

- Leon Battista Alberti
  - 15th century Florentine polymath -- painter, poet, composer, philosopher, author of the treatise *De pictura* (On painting), which contained the first scientific analysis of perspective
  - He was best known as an architect -- designed Rome's Trevi Fountain, and wrote the first printed book on architecture, *De Re Aedificatoria*
  - Around 1460, prompted by a casual conversation about cryptography in the Vatican gardens with Leonardo Dato, the pontifical secretary, he wrote an essay on the subject, outlining what he believed to be a new form of cipher -- the first polyalphabetic cipher, that used a cipher disk

# The Beginnings of Modern Cryptography






- Johannes Trithemius
  - 15th century German abbot. born Johann Heidenberg in Trittenheim on the Mosel
  - Major works include *Steganographia*, written circa 1499, *Polygraphiae*, a cryptographic work and *De Septum Secundis*, a history of the World based on astrology, both of which were published in 1508.
  - *Polygraphiae* was the first printed book on cryptography

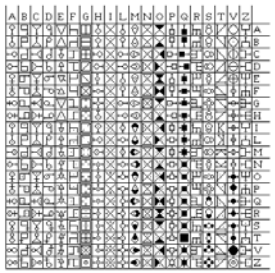


# The Beginnings of Modern Cryptography

- Giovan Batista Belaso
  - Not much known about him:
    - Came from Brescia (Italy)
    - Served in the suite of Cardinal Carpi
    - In 1533, in a small booklet entitled *La cifra del. Sig. Giovan Batista Belaso*, proposed the idea of using a pass-phrase as the key for a polyalphabetic cipher



# The Beginnings of Modern Cryptography



- Giovanni Battista Porta (1535-1615)
  - Born in Naples
  - In 1563, published *De Furtivis Literatum Notis*, containing the first digraphic cipher (one in which two letters are represented by a single symbol)
  - He also suggested the use of synonyms and misspellings to irritate cryptoanalysts



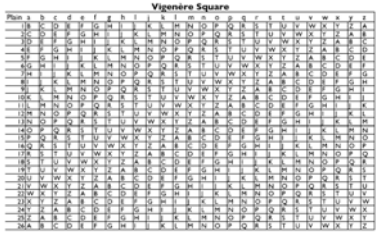
# The Beginnings of Modern Cryptography

- Blaise de Vigenère (1523-1596)
  - Born in the village of Saint-Pourçain, about halfway between Paris and Marseilles
  - Became steeped in cryptography during his diplomatic missions to the Vatican
  - In 1585, wrote *Traicté des Chiffres*, ("A Treatise on Secret Writing") which distilled much of cryptographic lore at the time, and was the first European representation of Japanese ideograms.
  - He discussed polyalphabetic ciphers using a Trethemius-like tableau, and an autokey* cipher system

*An *autokey* cipher is one which incorporates the message into the key

# The Beginnings of Modern Cryptography

- Blaise de Vigenère (1523-1596)
  - Inventor of the first acceptable autokey cipher system (the first, an imperfect one, was invented by Girolamo Cardano, a Milanese physician and mathematician)
  - He is most famous for the *Vigenère Cipher*, which employs only standard alphabets and a short repeating keyword -- it is far less secure than his autokey cipher.
  - It uses a *Tabula recta*, a cryptographic term invented by Johannes Trithemius in 1518
  - The *Vigenère Cipher* was thought for a time to be unbreakable (*Le Chiffre Indéchiffrable* -- "The Indecipherable Cipher")






# The Beginnings of Modern Cryptography

- The Great Cipher of Louis XIV (17th century)
  - Used by Louis to encrypt his most secret messages
  - Invented by father-and-son team, Antoine and Bonaventure Rossignol
  - So secure that it defied all attempts at breaking it, until 1890, when Victor Gendron, a military historian researching the campaigns of Louis XIV, came across a series of enciphered letters. He gave them to Commandant Étienne Bazeries, a distinguished expert in the French Army's Cryptographic Department, who broke the code after much effort.
  - It seemed to solve one of the great mysteries of the 17th century: The true identity of the *Man in the Iron Mask* (although there are still questions to this day)

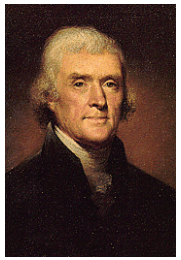


# The Beginnings of Modern Cryptography

- The Black Chambers (18th century)
  - By the 18th century, cryptanalysis was becoming industrialized
  - Each European power had its own so-called *Black Chamber*, for deciphering messages and gathering intelligence
  - The most celebrated Black Chamber was the *Geheime Kabinets-Kanzlei*, in Vienna.
  - England had its black chamber, headed by John Wallis (1616 - 1703), the greatest English mathematician before Isaac Newton



# The Beginnings of Modern Cryptography



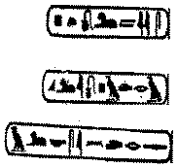
- Thomas Jefferson (1743 - 1826)
  - Writer, agriculturalist, bibliophile, architect, diplomat, gadgeteer, statesman, and third President of the United States
  - Invented his "Wheel Cypher" in the 1790s
  - Far and away the most advanced of its day
  - In 1922, the U.S. Army adopted an almost identical device that had been independently invented; it was used for at least 40 years.
  - Confers on Jefferson the title of Father of American Cryptography.

# The Rosetta Stone

- For 1400 years, no one knew how to read Egyptian hieroglyphics
- In 1799, a Napoleonic French soldier found a black basalt stone slab near an Egyptian town, Rosetta.
- It was carved with inscriptions in three different scripts: Egyptian hieroglyphics, demotic script (a late cursive form of hieroglyphics) and Greek.
- The stone bore a decree from the general council of Egyptian priests issued in 196 B.C.
- When the French surrendered to the British in Egypt, the British took possession of the stone, and it was shipped to the British Museum, where it remains to this day



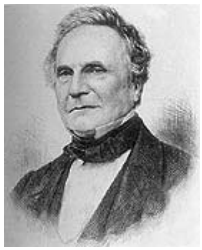
# The Rosetta Stone



- Many people tried to decipher the contents of the stone, until Jean-Francois Champollion (1790-1832), by building on the work of others, by adding his own brilliant and original assumptions, and after 14 years of study
- Champollion concluded that hieroglyphics had originally been pictographs, but phonetically based.
- He found many homophones (different signs standing for the same sound)



# The Beginnings of Modern Cryptography



- Charles Babbage (1791 - 1871)
  - In about 1854, developed the method of statistical analysis by which he successfully decrypted messages encrypted by the Vigénere square.
  - Unfortunately, due to his habit of not completing ‘the paperwork’, or possibly to protect the fact that, because of his work, Britain could decrypt Vigénere encrypted messages sent in the Crimea, this fact was not discovered until the twentieth century.



# The Beginnings of Modern Cryptography

- Friedrich Wilhelm Kasiski (1805-1881)
  - The honor of developing the statistical attack technique and cracking Vigénere was to go to a retired Prussian Army officer, who published it in *Die Geheimschriften und die Dechiffrir-kunst* ("Secret Writing and the Art of Deciphering"), written in 1863
  - The technique consisted of finding the length of the keyword and then dividing the message into that many simple substitution cryptograms. Frequency analysis could then be used to solve the resulting simple substitutions.
  - This technique has since been termed the *Kasiski Test*
  - Babbage beat him to it, but no one knew until much later.

# The Beginnings of Modern Cryptography

- Cryptography becomes popular
  - In the 19th century, the public became familiar with cryptography:
    - "Agony columns"
    - Cryptographers would insert ciphertext into newspapers merely to challenge their colleagues
    - Jules Verne's *Journey to the Center of the Earth* refers to the decipherment of a parchment filled with runic characters
    - Sir Arthur Conan Doyle's detective, Sherlock Holmes, was an expert in cryptography, as shown in the *Adventure of the Dancing Men* (see web site), which involves a cipher consisting of stick men, each representing a distinct letter:



# The Beginnings of Modern Cryptography

- Cryptography becomes popular
  - Edgar Allan Poe also developed an interest in cryptanalysis
  - He issued a challenge to the readers of Philadelphia's *Alexander Weekly Messenger*, claiming that he could decipher any monoalphabetic substitution cipher; he successfully deciphered all of the hundreds of submissions.
  - In 1843, he wrote a short story, *The Gold Bug*, which is widely acknowledged by professional cryptographers to be the finest piece of fictional literature on the subject of cryptography. (See web site)




# The Beginnings of Modern Cryptography

- Sir Charles Wheatstone (1802 - 1875)
  - Constructed an electric telegraph before Morse; Invented the concertina; Improved the dynamo; studied underwater telegraphy; Popularized a method for extremely accurate measurement of electrical resistance known as the "Wheatstone bridge", etc., etc., etc...
  - Fellow of the Royal Society; friend of Charles Babbage
  - Around 1860, deciphered a long cipher letter of Charles I
  - Displayed his *Cryptograph* at the Exposition Universelle at Paris in 1867
  - More important was his invention of the *Playfair cipher*, who he named after his friend, Lyon Playfair, the first Baron Playfair of St. Andrews; the first literal digraphic cipher (Porta's earlier digraphic cipher was symbolic, not literal)



# The Beginnings of Modern Cryptography

- Auguste Kerckhoffs (1835-1903)
  - Born Jean-Guillaume-Hubert-Victor-Francois-Alexandre-August Kerckhoffs von Nieuwenhof (*phew!*) at Nuth, Holland
  - Worked in France, where cryptography was active at the time
  - In 1883, wrote *La Cryptographie militaire*, the second great book on cryptography, after that of Porta.
  - Enunciated *Kerckhoffs' law*, the principle that the security of a cryptosystem must depend only on the ***key***, not on the secrecy of any other part of the system.

# The Beginnings of Modern Cryptography

- Herbert Osborne Yardley (1889 - 1958)
  - Born in Worthington, Indiana
  - In 1912, obtained a job in Washington, D.C. as a State Department telegraph operator, where he played games decoding messages to President Woodrow Wilson
  - Tried to convince his superiors that the American codes at that time were hopelessly outdated, but only when World War I broke out did the government do anything
  - Was named head of a special cryptographic bureau called MI8 (Military Intelligence, Section 8)



# The Beginnings of Modern Cryptography

- Herbert Osborne Yardley (1889 - 1958)
  - Within months, MI8 had broken almost all the German diplomatic and Abwehr (defense) codes.
  - Yardley deciphered a letter which caused Lothaw Witzke, a German saboteur, to be tried, convicted, and sentenced to death (later reprieved by President Wilson)
  - In 1918, went to Europe to learn more about British and French cryptographic methods



# The Beginnings of Modern Cryptography

- Herbert Osborne Yardley (1889 - 1958)
  - When told, after the end of WWI, that his organization was no longer needed, he strenuously disagreed, writing a report *Code and Cipher Investigation and Attack*
  - People were impressed, and so an "unofficial" code breaking operation was formed, with Yardley at the head
  - Yardley called the organization the *American Black Chamber*
  - Was successful in breaking various difficult codes, and in particular was able to break the Japanese diplomatic codes, so the Americans were able to successfully negotiate against the Japanese at the 1921 Washington Naval Conference



# The Beginnings of Modern Cryptography

- Herbert Osborne Yardley (1889 - 1958)
  - In 1924, the State Department considerably reduced MI8's funds, under direct orders from President Calvin Coolidge.
  - In 1928, Henry L. Stimson was appointed Secretary of State, and he ordered MI8 out of business, saying "Gentlemen to not read each other's mail"
  - Yardley had ruffled too many feathers, and found himself unemployable. Eventually, he wrote a book, *The American Black Chamber*, which talked about how the codes had been broken, and was very popular.
  - Congress and other cryptologists were perturbed, and congress passed a new law prohibiting federal employees from revealing government secrets

# The Beginnings of Modern Cryptography

- Herbert Osborne Yardley (1889 - 1958)
  - Yardley wrote several more books, turning to fiction to write a spy-comedy, *The Blonde Countess*. This, and elements from *The American Black Chamber*, made up the script for the 1935 movie *Rendezvous*, starring William Powell and Rosalind Russell
  - In 1938, Yardley went to China, working for Chiang Kai-shek's intelligence bureau, to crack the codes of the Japanese army, who were then invading China
  - By 1941, he had moved to Canada to help form a code-breaking bureau
  - When WWII broke out, he returned to the U.S., where he was given a low-level paper-shuffling job; amazingly, the government did not feel it wanted his talents in any cryptographic context!



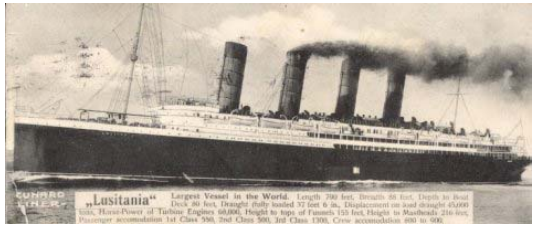
# World War I

- German ADFGVX Cipher
  - Introduced in March, 1918, just before the German offensive against France
  - The French were forced to break the cipher, in order to defend themselves
  - The cipher was broken by Lieutenant Georges Painvin, which allowed the French to learn what the Germans were planning, and thus the Germans lost the element of surprise.



# The Zimmerman Telegram

- President Woodrow Wilson spent 2 years of WWI refusing to send American troops to support the Allies
- In 1915, a submerged German U-boat had sunk the ocean liner Lusitania, drowning 1,198 passengers, including 128 U.S. civilians
- The loss of the Lusitania would have brought the U.S. into the war, except that Germany reassured them that henceforth U-boats would surface before attacking






# The Zimmerman Telegram

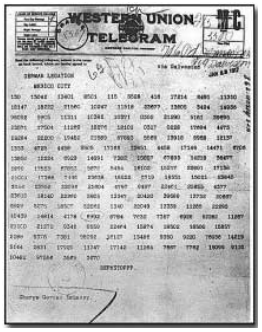
- In 1916, Germany appointed a new Foreign Minister, Arthur Zimmerman, who persuaded the U.S. not to come into the war.
- Germany decided to change the U-boat policy and return to underwater attacks, but needed to distract the U.S. so as not to cause them to enter the war.

# The Zimmerman Telegram

- Zimmerman proposed an alliance with Mexico and to persuade the President of Mexico to invade the U.S. to reclaim territories such as Texas, New Mexico, and Arizona
- He also wanted the Mexican president to act as a mediator and persuade Japan to attack the U.S. from the west.
- With such problems at home, it was expected that the U.S. could not afford to send troops to Europe.



# The Zimmerman Telegram




- Zimmerman sent his proposal in the form of an enciphered telegram to the German Ambassador in Washington, who would retransmit it to the German Ambassador to Mexico, who would deliver it to the Mexican President
- The telegram was intercepted by the British, who sent it to their "Room 40", the Admiralty cipher bureau, who eventually deciphered it.
- After some delay, the British conveyed the deciphered message to the Americans, who as a result recognized the duplicity of the Germans, and entered the war.



# The Beginnings of Modern Cryptography

- William Reginald Hall (a.k.a. Blinker) (1870 - 1943)
  - Raised in Wiltshire, England
  - His father was made the first director of the Foreign Intelligence Committee in 1883
  - Hall was named director of naval intelligence in 1914
  - The Magdeburg codebook had been captured early in WWI, which allowed the British to know the position of every German ship throughout the entire war.
  - Hall's greatest coup was to decipher the Zimmerman Telegram
  - After WWI, Hall was elected a Member of Parliament.



# Enigma

- In 1918, German inventor Arthur Scherbius devised an electrical equivalent of Alberti's cipher disk. It was a machine based on revolving wired codewheels, or rotors.
- He called it Enigma, and offered it to the German military, who eventually adopted it, after they learned how important cryptography had been to the Allies in WWI
- Enigma was the most secure cryptographic system devised at that time; Scherbius calculated that if 1,000 cryptographers, each with a captured Enigma, tested 4 keys/minute, all day, every day, it would take 1.8 billion years to try them all.

# Enigma

- In 1920, Poland, threatened by Russia from the east, and Germany from the west, created a cryptanalytic section in its Army General Staff -- the *Biuro Szyfrow* (Cipher Bureau)
- The Biuro was determined to break Enigma, and so recruited a group of young mathematicians
- Marian Rejewski and others started work on cracking Enigma

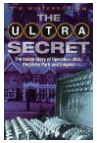


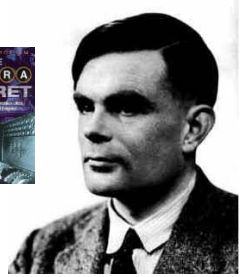
# Enigma

- Hans-Thilo Schmidt, a discontented employee of the German Army cipher bureau offered the French the operational manuals for Enigma. The French passed copies to the Poles.
- After much effort, the Poles managed to break the Enigma code, but deciphering was very time-consuming, and whenever the Germans changed the Enigma configurations they had to work hard to compensate.
- Eventually, they were unable to keep pace with the German changes, but they informed the British and the French of their successes, and this encouraged the Allies to continue the work.



# Enigma



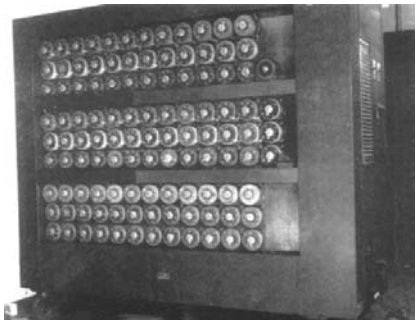



- The British set up a new cryptographic section, in Bletchley Park, Buckinghamshire
- They recruited a very diverse group of people: linguists, classicists, chess players, mathematicians and scientists
- The most famous of these people was Alan Turing
- Through immense effort and brilliance, they succeeded in consistently deciphering Enigma coded messages, and had an enormous effect on shortening WW2



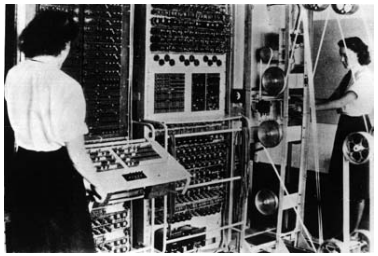
# Enigma

- Turing invented a machine -- a "bombe" to assist with the decipherment; it was manufactured by the British Tabulating Machine Company in Letchworth, Hertfordshire



# Enigma

- In January 1943, along with a number of colleagues, Turing began to construct an electronic machine to decode the Enigma cipher. This machine, which they dubbed COLOSSUS, comprised 1,800 vacuum tubes and was completed and working by December of the same year!
- By any standards, COLOSSUS was one of the world's *earliest working programmable electronic digital computers*.





# Enigma

- Unfortunately, because of government secrecy, the fact that they were essentially the first to design and construct a programmable computer wasn't known until much later when Group Captain Frederick William Winterbotham published the book *The Ultra Secret*, in 1974.
- Among many revelations, the book revealed that the British had to be very careful not to act on every deciphered message, so as not to give the game away to the Germans:
  - In 1940, the German Air Force bombed Coventry, England, where many factories were producing aircraft for the war effort. The city suffered major damage, including the destruction of the cathedral, which dated back to 1043, and considerable civilian casualties
  - The British had advance warning of the attack, but chose to sacrifice those lives rather than reveal to the Germans that they had cracked Enigma.
  - This was but one of many such cases.



# The Beginnings of Modern Cryptography

- William Frederick Friedman (1891 - 1969)
  - Born Wolfe Friedman in Kishinev, Russia; emigrated to the U.S. in 1892
  - Was hired by George Fabyan's Riverbank Laboratories to try to prove that Francis Bacon wrote Shakespeare's plays.
  - In 1917, married Elisebeth (sic) Smith, also a cryptologist at Riverbank



# The Beginnings of Modern Cryptography


- William Frederick Friedman (1891 - 1969)
  - In the late 1930s, was asked to work on the Japanese master code, known as *Purple*
  - Purple, like Enigma, was an electromechanical cipher which accepted typewritten input (in Latin letters) and produced ciphertext output
  - Purple was broken by a team from the US Army Signals Intelligence Service, then directed by Friedman
  - The information gained from decryptions was eventually code-named *Magic* within the U.S. government.

# The Beginnings of Modern Cryptography

- William Frederick Friedman (1891 - 1969)

  - US cryptographers decrypted and translated the 14-part Japanese diplomatic message declaring war against the States before the Japanese Embassy in Washington could.
  - The U.S. never found any hint of the attack on Pearl Harbor in the Purple traffic because the Japanese were very careful to not discuss the planned attack in Foreign Office communications
  - The ability to read Japanese messages brought about many decisive American naval victories, including the battles of the Coral Sea and Midway.



# The Beginnings of Modern Cryptography

- William Frederick Friedman (1891 - 1969)
  - Visited Bletchley Park in 1941, and exchanged information on his code-breaking techniques that had penetrated Purple, together with learning how the British had cracked Enigma
  - After WWII, Friedman became the chief cryptologist for the National Security Agency (NSA)
  - Considered to be the greatest American cryptologist



# Linear B

- In 1900, the British archaeologist Sir Arthur Evans (1851-1941) discovered and escavated Knossos, the site of the palace of King Minos, on Crete, famous for the Labyrinth of the Minotaur
- He discovered a large number of clay tablets inscribed with mysterious symbols.
- He realised that the inscriptions represented three different writing systems: a 'hieroglyphic' script, Linear A, and Linear B.




# Linear B

- Linear B is the oldest surviving record of the Greek dialect known as Mycenaean, named after the Greek site of Mycenae, where the legendary Agamemnon ruled.
- The script's usage spanned the time period between ~1500 BC and 1200 BC, and geographically covered the island of Crete, as well as the southern part of the Greek mainland.
- It took until 1953, when Michael Ventris (1922-1956) eventually deciphered Linear B
- Later, with the help of John Chadwick, an expert on early Greek, he showed beyond reasonable doubt the Linear B did indeed represent Greek.

# Microdots

- A Microdot is a page of text, photographically shrunk down to a dot less than a millimeter in diameter
- The first microdot to be spotted by the FBI was in 1941
- Thereafter, the Americans could read the contents of most intercepted microdots, except when the contents had been already encrypted.



# The Code Talkers

- Lacking secure battlefield voice communications during WWI, the U.S. Army had employed Choctaws to encrypt voice communications, using their native language, itself encoded.
- The Army studied the program even before the U.S. entered WWII in 1941, and during World War II employed Commanches, Choctaws, Kiowas, Winnebagos, Seminoles, Navajos, Hopis, Cherokees and others.
- The Marine Corps took the Army work and codified, expanded, refined and perfected it into a true security discipline, using Navajos exclusively. In campaigns against the enemy on many fronts, the Native American Code Talkers never made a mistake in transmission nor were their codes ever broken.
- (See: http://www.nsa.gov/museum/navajomonograph.pdf )



# The National Security Agency (NSA)


- Came into existence after the investigation of the surprise attack of the Japanese on Pearl Habor, which showed that the different arms of the U.S. armed forces were not sharing security matters.
- In 1949, the U.S. Defense Dept. established the Armed Forces Security Agency (AFSA)
- In 1952, President Harry S. Truman produced a directive that created the the NSA and abolished AFSA
- For several years, that directive was classified, and the U.S. government did not publicly acknowledge the existence of the agency



# The National Security Agency (NSA)

- Finally, in 1957, the United States Government Organization Manual included a brief but vague description
- Today, the NSA is still a somewhat shadowy organization, but it does now have a web site! (**http://www.nsa.gov/**)
- It is the largest security organization in the world, and probably employs more cryptographers than anyone else -- by a wide margin; probably among the best in the world
- It is suspected that NSA has cracked a number of important ciphers, but since they never publicize their exploits, it's hard to tell rumors from the truth

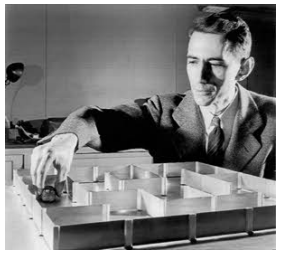
# The Data Encryption Standard (DES)

- In the 1960s and early 1970s it started to become apparent that there was a need for a standard encryption mechanism to allow multiple organizations (mostly commercial) to communicate securely.
- In 1973/4, the National Bureau of Standards (NBS) -- later known as the National Institute of Standards and Technology (NIST) -- solicited candidate cryptosystems in the Federal Register
- A handful of proposals were submitted
- One was based on a cryptosystem devised by Horst Feistel of IBM, which in turn was based on the mathematical foundations created by Claude Shannon



# The Data Encryption Standard (DES)

- Claude Elwood Shannon (1916 - 2001)



  - Born in Petoskey, Michigan, and attended the University of Michigan, graduating in 1936 with bachelor's degrees in mathematics and electrical engineering.
  - Obtained a Master's degree in electrical engineering and a Ph.D. in mathematics from MIT in 1940; his doctoral thesis was on population genetics



# The Data Encryption Standard (DES)

- Claude Elwood Shannon (1916 - 2001)
  - Joined AT&T Bell Telephones in New Jersey in 1941 as a research mathematician and remained at the Bell Laboratories until 1972.
    - *"... became known for keeping to himself by day and riding his unicycle down the halls at night."*
  - Published *A Mathematical Theory of Communication* in the *Bell System Technical Journal* (1948). This paper founded the subject of information theory
  - In 1949, published a paper entitled *Communication Theory of Secrecy Systems*. This work is now generally credited with transforming cryptography from an art to a science.



# The Data Encryption Standard (DES)

- Claude Elwood Shannon (1916 - 2001)
  - Returned to MIT in 1958
    - *"... continued to threaten corridor-walkers on his unicycle, sometimes augmenting the hazard by juggling."*
    - *"... had a whimsical side and developed a juggling machine, rocket-powered Frisbees, motorized Pogo sticks, a mind-reading machine, a mechanical mouse that could navigate a maze and a device that could solve the Rubik's Cube puzzle."*

# The Data Encryption Standard (DES)

- Horst Feistel
  - Immigrated to the U.S. from Germany in 1934
  - Was placed under house arrest when WWII broke out, until 1944
  - Began research into ciphers at the U.S. Air Force's Cambridge Research Center, but ran into trouble with NSA, because NSA wanted a monopoly on cryptographic research
  - In the 1960s, moved to the Mitre Corporation, but ran afoul of the NSA again
  - Eventually, Feistel moved to IBM's Thomas J. Watson Laboratory, near New York. It was there he developed the *Lucifer* system



# The Data Encryption Standard (DES)

- Horst Feistel
  - In May, 1973, Feistel published a Scientific American article *Cryptography and Computer Privacy*

SCIENTIFIC AMERICAN

Cryptography and Computer Privacy

*Computer systems in general and personal "data banks" in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer*

by Horst Feistel



# The Data Encryption Standard (DES)

- Horst Feistel
  - Feistel was familiar with computer technology and with binary digital form, which he used heavily
  - The Lucifer cipher he devised was sufficiently complex that it could not reasonably be implemented by hand; only in a computer
  - Lucifer was an example of a *block cipher*, operating on fixed size blocks of plaintext bits
    - A block cipher encrypts a batch of plaintext symbols into an equal length of ciphertext symbols.
    - The advantage of a block cipher is diffusion where bits or bytes are dispersed throughout the cipher text such that a single change of one bit affects the position of multiple bits during subsequent rounds.



# The Data Encryption Standard (DES)

- Horst Feistel
  - Lucifer became known as one of the strongest commercially available cryptosystems, and so was used by a variety of organizations
  - IBM submitted it as a proposal to NBS
  - However, NSA interfered again, and required that the strength of the cipher be reduced to 56 bits (the number of possible keys would be roughly 100,000,000,000,000,000, which consumes 56 bits); NSA did not want an encryption standard which they could not break
  - This version was officially adopted on Nov 23, 1976, and was called the *Data Encryption Standard (DES)*, but not without some major questions regarding the NSA's motives

# Public Key Cryptography

- A major longstanding problem with private key ciphers:
  - How to securely exchange a key between people or organizations who wished to communicate with each other in a secure fashion?
- This is called the *Key Distribution Problem*, and was a major issue:
  - Large amounts were being spent physically carrying keys, or codebooks containing all the keys for, say, a month
  - During WWII, the German High Command had to distribute the monthly book of day keys to all its Enigma operators – an enormous logistical problem, and one that involved a potential security risk

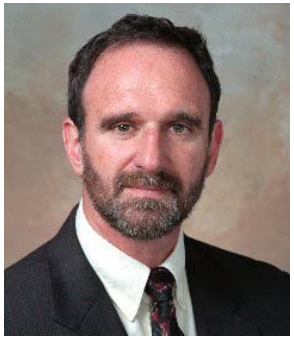


# Public Key Cryptography

- Whitfield Diffie (1944 - )
  - Graduated from MIT in 1965 with a B.S. in Mathematics
  - Then took a series of jobs relating to computer security, becoming a freethinking cryptographer – the first "cypherpunk"
  - Became interested in the key distribution problem
  - In 1974, gave a talk at IBM's Thomas J Watson Lab, and learned that Martin Hellman had just given a talk there about the problem of key distribution
  - Now at Sun Microsystems



# Public Key Cryptography



- Martin Hellman (1945 - )
  - Born in the Bronx, NY, and graduated with a B.S. in 1966 from New York University
  - Received M.S. and Ph.D. from Stanford University
  - Was a researcher at IBM's Watson Research Center from 1968-69 and an Assistant Professor of Electrical Engineering at MIT from 1969-71.
  - Has been at Stanford University since 1971, becoming Professor Emeritus in 1996



# Public Key Cryptography

- Diffie drove across the U.S. to meet Hellman, and managed to obtain a graduate student position so that the two could work together
- Diffie and Hellman studied the key distribution problem, and were later joined by Ralph Merkle

# Public Key Cryptography

- Ralph C. Merkle
  - Received his PhD in 1979 from Stanford
  - Worked with Diffie and Hellman
  - He joined Xerox PARC in 1988, pursuing research in computational nanotechnology.
  - Now Distinguished Professor of Computing at Georgia Tech College of Computing, and Director, Georgia Tech Information Security Center
  - Is now heavily into nanotechnology, having won awards in the field



# Public Key Cryptography

- Diffie came up with the idea of an *asymmetric-key cryptography* (a.k.a. *public-key cryptography*) in 1975
  - Uses two related keys: one *public key*, and one *private key*
  - Either key can be used to encrypt a message; the other decrypts it
- He published an outline of his idea in the summer of 1975
- He had not yet come up with a workable, practical implementation



# Public Key Cryptography

- They finally came up with a solution to the key exchange problem in 1976: The *Diffie-Hellman-Merkle Key Exchange Scheme* (often shortened to just *Diffie-Hellman*), which allows the establishment of a secret through a public exchange
- They publicly demonstrated their discovery at the National Computer Conference in June 1976, where it caused a sensation in the cryptographic community
- Still, there needed to be a practical implementation



# Public Key Cryptography

- Ron Rivest, Adi Shamir, Leonard Adleman (RSA)
  - Working at MIT's Laboratory for Computer Science, came up with the first practical asymmetric cipher
  - They called it RSA, after the initials of their last names
  - Announced in August, 1977, by Martin Gardner in Scientific American, who issued a challenge to readers to break a ciphertext that he published (he also provided the key he had used to encrypt it). The prize was $100, and it took 17 years before the ciphertext was broken.
  - In April, 1994, a team of 600 volunteers announced that they had broken the cipher; they had used spare time on their computers spread across several continents.

# Public Key Cryptography

- There was a parallel history of events:
  - After WWII, the remnants of Bletchley Park in the U.K. were reformed into the Government Communications Headquarters (GCHQ), and moved to Cheltenham, in Gloucestershire. GCHQ operated under very strict security measures
  - In the late 1960s, they also started to worry about the issue of key distribution, and in 1969, asked James Ellis to look into the problem.



# Public Key Cryptography

- James Ellis (? – 1997)
  - Grew up in the East End of London in the 1920s
  - Studied physics at Imperial College, London
  - Joined Post Office Research Station at Dollis Hill, where Tommy Flowers had built Colossus
  - In 1965, absorbed into Communications-Electronics Security Group, a section of GCHQ
  - Inspired by an anonymous Bell Telephone paper, produced a memo in 1969 which essentially came up with the same idea as Diffie, Hellman and Merkle.
  - Everything at GCHQ was top secret, so he couldn't publish it



# Public Key Cryptography

- Clifford Cocks, Malcolm Williamson
  - GCHQ mathematicians who followed up on Ellis' work
  - In 1973, Cocks produced the approximate equivalent to RSA
  - In 1974, Williamson discovered an algorithm that was very similar to the work of Diffie and Hellman
  - It was only in 1997 that the British Government released information about the GCHQ pioneering work, which had previously been classified.



# Pretty Good Privacy

- Phil Zimmerman
  - Was an anti-nuclear activist
  - When the Cold War ended, became convinced that everyone's privacy was at risk if they did not have easy access to strong cryptography
  - In the late 1980s, wrote a software package which provided an easy user interface to strong cryptography; he called it *Pretty Good Privacy (PGP)*
  - In 1991, asked a friend to post PGP on a Usenet bulletin board

# Pretty Good Privacy

- PGP took off on the Internet, especially abroad
  - Human rights groups started using it to prevent information from falling into the hands of regimes they were accusing of human rights abuses
  - Resistance groups in Burma
  - In the Soviet Union, during its breakup



# Pretty Good Privacy


- However, certain groups in the U.S. had problems with his actions:
  - In 1993, two government investigators paid him a visit, questioning him about his "illegal exportation of a weapon"
  - Was investigated by the FBI, and became the subject of a grand jury investigation
  - Finally, in 1996, the U.S. Attorney General's Office dropped the investigation, basically giving up the fight
- Steven Levy wrote a book *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*

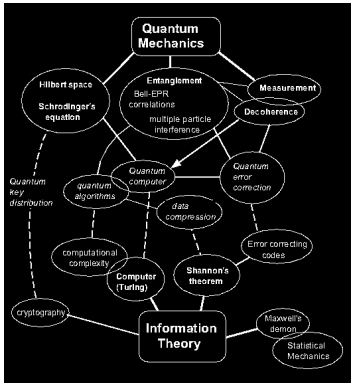


# The Advanced Encryption Standard (AES)

- After DES had been broken, it was apparent that, with the availability of cheaper and faster hardware, DES would be rendered untenable in a few years.
- In 1997, NIST issued a Request For Comment (RFC) for a standard -- to be called the *Advanced Encryption Standard (AES)* -- to replace DES
- In response, a number of submissions were received, and one was selected:
  - "Rijndael" by Joan Daemen and Vincent Rijmen, two Belgian cryptographers
- AES (Rijndael) is now, as of Nov 2001, a Federal Information Processing Standard (FIPS)
- Details on AES (Rijndael) may be found at the web page http://csrc.nist.gov/CryptoToolkit/aes/



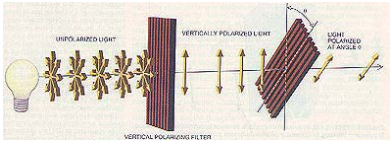
# Quantum Cryptography




- In 1985, David Deutsch, a British physicist published a paper which described his ideas on the theory of computers based on the laws of quantum physics: a *quantum computer*
- In theory, a quantum computer could easily decipher even strongly encrypted messages in very little time; of course, this generates lots of interest...
- See: http://www.qubit.org/library/intros/compSteane/qcintro.html

# Quantum Cryptography

- In the late 1960s, Stephen Wiesner, a graduate student at Columbia University came up with the idea of *quantum money*
- 14 years later, this inspired Charles Bennett and Gilles Brassard to invent an absolutely secure system of communication: *quantum cryptography*
  - not relatively secure, but *absolutely* secure, based on the laws of quantum physics, the most successful physical theory ever
- In 1988, Bennett and John Smolin achieved the first quantum cryptographic exchange






# The End of Cryptographic History?

- If quantum cryptography systems can be engineered to operate over long distances, then the evolution of ciphers will stop, because it will an absolutely secure system
- But will governments allow us to use that technology?