Cryptography Made Easy

Stuart Reges
Senior Lecturer
Why Study Cryptography?

• Secrets are intrinsically interesting
• So much real-life drama:
  – Mary Queen of Scots executed for treason
  – primary evidence was an encoded letter
  – they tricked the conspirators with a forgery
• Students enjoy puzzles
• Real world application of mathematics
Start with an Algorithm

• The Spartans used a scytale in the fifth century BC (transposition cipher)
• Card trick
• Caesar cipher (substitution cipher):
  
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
  GHIJKLMNOPQRSTUVWXYZABCDEF
  GHIJKLMNOPQRSTUVWXYZABCDEF
Then add a secret key

- Both parties know that the secret word is "victory":
  
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
  VICTORYABDEFGHJKLMNPQRSTUVWXZ

- "state of the art" for hundreds of years
- Gave birth to cryptanalysis first in the Muslim world, later in Europe
Cryptographers vs Cryptanalysts

• A battle that continues today
• Cryptographers try to devise more clever algorithms and keys
• Cryptanalysts search for vulnerabilities
• Early cryptanalysts were linguists:
  – frequency analysis
  – properties of letters
Vigenère Square (polyalphabetic)

| 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 | 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 |
| 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 |
| 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 Vigenère Square is a polyalphabetic substitution cipher that uses a repeating keyword to shift the alphabet. Each row and column represents a different Caesar cipher, and the intersection of the row and column is the encrypted letter.
Vigenère Cipher

- More secure than simple substitution
- Confederate cipher disk shown (replica)
- Based on a secret keyword or phrase
- Broken by Charles Babbage
Cipher Machines: Enigma

- Germans thought it was unbreakable
- Highly complex
  - plugboard to swap arbitrary letters
  - multiple scrambler disks
  - reflector for symmetry
- Broken by the British in WW II (Alan Turing)
Public Key Encryption

- Proposed by Diffie, Hellman, Merkle
- First big idea: use a function that cannot be reversed (humpty dumpty)
- Second big idea: use asymmetric keys (sender and receiver use different keys)
- Key benefit: doesn't require the sharing of a secret key
RSA Encryption

-Named for Ron Rivest, Adi Shamir, and Leonard Adleman
-Invented in 1977, still the premier approach
-Based on Fermat’s Little Theorem:
  \[ a^{p-1} \equiv 1 \pmod{p} \text{ for prime } p, \gcd(a, p) = 1 \]
- Slight variation:
  \[ a^{(p-1)(q-1)} \equiv 1 \pmod{pq} \text{ for distinct primes } p \text{ and } q, \gcd(a,pq) = 1 \]
-Requires large primes (100+ digit primes)
Example of RSA

- Pick two primes $p$ and $q$, compute $n = p \times q$
- Pick two numbers $e$ and $d$, such that:
  $$e \times d = k(p-1)(q-1) + 1$$ (for some $k$)
- Publish $n$ and $e$ (public key), encode with:
  $$(\text{original message})^e \mod n$$
- Keep $d$, $p$ and $q$ secret (private key), decode with:
  $$(\text{encoded message})^d \mod n$$
Why does it work?

- Original message is carried to the e power, then to the d power:
  \[(msg^e)^d = msg^{e \cdot d}\]

- Remember how we picked e and d:
  \[msg^{ed} = msg^{k(p-1)(q-1) + 1}\]

- Apply some simple algebra:
  \[msg^{ed} = (msg^{(p-1)(q-1)})^k \times msg^1\]

- Applying Fermat's Little Theorem:
  \[msg^{ed} = (1)^k \times msg^1 = msg\]
Politics of Cryptography

- British actually discovered RSA first but kept it secret
- Phil Zimmerman tried to bring cryptography to the masses with PGP and ended up being investigated as an arms dealer by the FBI and a grand jury
- The NSA hires more mathematicians than any other organization
Exploring further

- Simon Singh, *The Code Book*
- RSA Factoring Challenge (unfortunately the prizes have been withdrawn)
- Shor's algorithm would break RSA if only we had a quantum computer
- Java's BigInteger class has methods for isProbablePrime, nextProbablePrime, modPow
Card Trick Solution

- Given 5 cards, at least 2 will be of the same suit (pigeon hole principle)
- Pick 2 such cards: one will be hidden, the other will be the first card
- First card tells you the suit
- Hide the card that has a rank that is no more than 6 higher than the other (using modular wrap-around of king to ace)
- Arrange other cards to encode 1 through 6
Encoding 1 through 6

• Figure out the low, middle, and high cards
  – rank (ace < 2 < 3 ... < 10 < jack < queen < king)
  – if ranks are the same, use the name of the suit
    (clubs < diamonds < hearts < spades)
• Some rule for the 6 arrangements, as in:
  1: low/mid/hi     3: mid/low/hi     5: hi/low/mid
  2: low/hi/mid     4: mid/hi/low     6: hi/mid/low