Math Rules Cyberspace

Travis H.

Morgen Academy Math Students, 23 May 2008

Web Sites

Castles on the Internet

- Have a practical purpose so can never be perfect
- More valuable the data, the stronger it must be
- Always under attack

Web Sites
Castles on the Internet

- Have a practical purpose so can never be perfect
- More valuable the data, the stronger it must be
- Always under attack

Web Sites

Castles on the Internet

- Have a practical purpose so can never be perfect
- More valuable the data, the stronger it must be
- Always under attack

Web Sites
Castles on the Internet

- Have a practical purpose so can never be perfect
- More valuable the data, the stronger it must be
- Always under attack

Firewalls
Keeping Bad Guys Out

- But a real firewall has to let *something* in or out
- Otherwise there's no point

What Really *Is* a Hacker?

- Most people only see superficial details
- A hacker wants to *understand* the Matrix
- Not necessarily malicious

System Crackers are Malicious Hackers

The Internet Ninjas

- Powers of invisibility
- Like to wear black
- Strike without warning
- Leave no trace
- Make most people uncomfortable

System Crackers are Malicious Hackers

The Internet Ninjas

- Powers of invisibility
- Like to wear black
- Strike without warning
- Leave no trace
- Make most people uncomfortable

System Crackers are Malicious Hackers

The Internet Ninjas

- Powers of invisibility
- Like to wear black
- Strike without warning
- Leave no trace
- Make most people uncomfortable

System Crackers are Malicious Hackers

The Internet Ninjas

- Powers of invisibility
- Like to wear black
- Strike without warning
- Leave no trace
- Make most people uncomfortable

System Crackers are Malicious Hackers

The Internet Ninjas

- Powers of invisibility
- Like to wear black
- Strike without warning
- Leave no trace
- Make most people uncomfortable

System Crackers are Malicious Hackers

The Internet Ninjas

- Powers of invisibility
- Like to wear black
- Strike without warning
- Leave no trace
- Make most people uncomfortable

Security Experts

Internet Jedi

- No effective law enforcement on Internet, like Wild West
- No regulation of software industry
- Nobody to protect people from vendors and crackers

Security Experts

Internet Jedi

- No effective law enforcement on Internet, like Wild West
- No regulation of software industry
- Nobody to protect people from vendors and crackers

Security Experts

Internet Jedi

- No effective law enforcement on Internet, like Wild West
- No regulation of software industry
- Nobody to protect people from vendors and crackers

There Are Temptations

Cryptologists
Modern Wizards

- Start off very weak
- Require many years to develop their powers
- Pore over dusty tomes to find the information they need
- Books are incomprehensible to others
- Full of weird symbols and obscure incantations

Cryptologists
Modern Wizards

- Start off very weak
- Require many years to develop their powers
- Pore over dusty tomes to find the information they need
- Books are incomprehensible to others
- Full of weird symbols and obscure incantations

Cryptologists
Modern Wizards

- Start off very weak
- Require many years to develop their powers
- Pore over dusty tomes to find the information they need
- Books are incomprehensible to others
- Full of weird symbols and obscure incantations

Cryptologists
Modern Wizards

- Start off very weak
- Require many years to develop their powers
- Pore over dusty tomes to find the information they need
- Books are incomprehensible to others
- Full of weird symbols and obscure incantations

Cryptologists
Modern Wizards

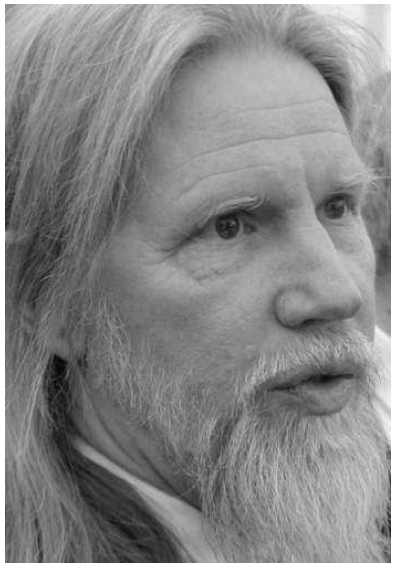
- Start off very weak
- Require many years to develop their powers
- Pore over dusty tomes to find the information they need
- Books are incomprehensible to others
- Full of weird symbols and obscure incantations

A Powerful Wizard

- Gandalf the White
- Most powerful wizard in Gondor

Coincidence? I think not.

- Gandalf the White
- Most powerful wizard in Gondor



- Whitfield Diffie
- Chief Security Officer at Sun Microsystems

Words of Wisdom

Do not meddle in the affairs of wizards, for they are subtle and quick to anger.

– J. R. R. Tolkein

Wizards **can** fight, but they **prefer** not to.

What All the Words Mean

cryptography is encrypting your information so that other people can't read it

cryptanalysis is trying to read other people's encrypted messages

cryptology is the study of both

What Makes a Good Cryptanalyst

- When I was about your age, I lived here in Texas
- My mother had a note on the calendar
- All it said was **N.B.**
- Can you figure out what she had planned?

Roman Times
The Skytale

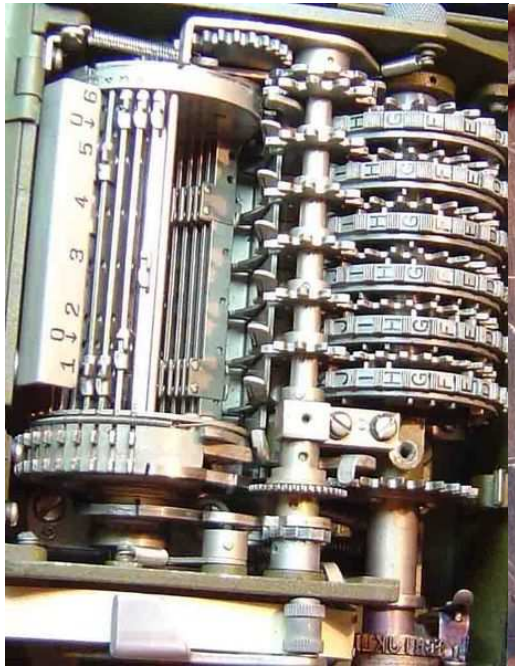
With Pencil and Paper

Until Eighty Years Ago

vigenere_square.svg

WW II through Korean War

HAGELIN M-209 CIPHER MACHINE (GVG / PD)



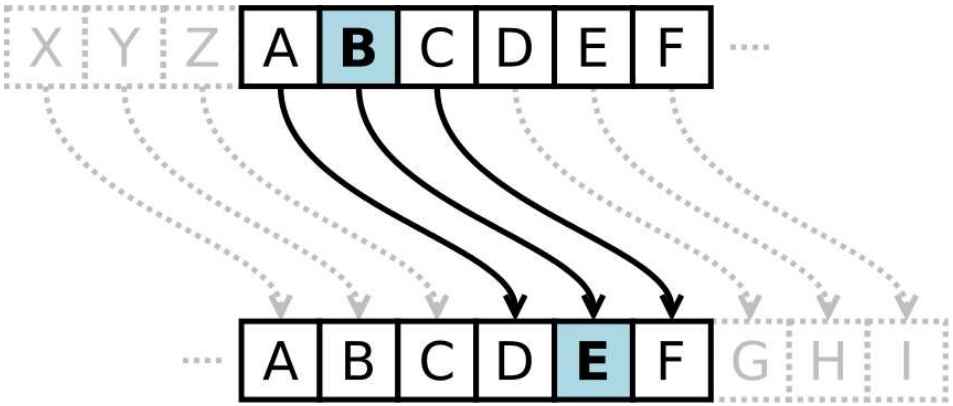
Late 20th Century
Russian Fialka Machine

Modern Encryption Machines

Almost Everything on the Internet

- If you see these icons, your computer is doing encryption

Caesar Cipher



Replace input (B) with letter three to the right (E)
The number three is called the *key* to the cipher
Wraps around
To decrypt we do the reverse
ANT becomes *DQW*

Caesar Cipher Example

substitution table

plaintext	ABCDEFGHIJKLMNOPQRSTUVWXYZ
ciphertext	DEFGHIJKLMNOPQRSTUVWXYZABC

example

plaintext	THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
ciphertext	WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

Changing Symbols

- We use 26 symbols (A-Z); this is called our *alphabet.*
- Nothing special about it
- For example, we could number them:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- These are called ordinal numbers.

Encrypting Using Numbers

- 1. Replace *A* with *0*, *B* with *1*, *C* with *2*, ... *Z* with *25*
- 2. Add the *key* (3) to each number
- 3. Replace *0* with *A*, *1* with *B*, *2* with *C*, ... *25* with *Z*
- But wait, what if we went over 25?
  - In that case we subtract 26 from the result
  - So 24 plus 3 is 27, but that's too high, so 27 - 26 = 1
  - This is called "modular addition".
- For decryption, we subtract the key *k*
  - If we go under zero, then we add 26

Encrypting Using Numbers

- 1. Replace *A* with *0*, *B* with *1*, *C* with *2*, ... *Z* with *25*
  2. Add the *key* (3) to each number
  3. Replace *0* with *A*, *1* with *B*, *2* with *C*, ... *25* with *Z*
- But wait, what if we went over 25?
  - In that case we subtract 26 from the result
  - So 24 plus 3 is 27, but that's too high, so 27 - 26 = 1
  - This is called "modular addition".
- For decryption, we subtract the key *k*
  - If we go under zero, then we add 26

Encrypting Using Numbers

- 1. Replace *A* with *0*, *B* with *1*, *C* with *2*, ... *Z* with *25*
  2. Add the *key* (3) to each number
  3. Replace *0* with *A*, *1* with *B*, *2* with *C*, ... *25* with *Z*
- But wait, what if we went over 25?
  - In that case we subtract 26 from the result
  - So 24 plus 3 is 27, but that's too high, so 27 - 26 = 1
  - This is called "modular addition".
- For decryption, we subtract the key *k*
  - If we go under zero, then we add 26

How Is This Math?

If x is the plaintext and y is the ciphertext, the equation we're using is:

$$y = (x + 3) \ mod \ 26$$

Or more generally, for a key k and an alphabet of n symbols:

$$y = (x + k) \ mod \ n$$

Decryption is similar:

$$x = (y - k) \ mod \ n$$

Cryptanalysis of Caesar Cipher

encrypted message

Nwcz akwzm ivl amdmv gmiza iow wcz nibpmza jzwcopb nwzbp wv bpqa kwvbqvmvb, i vme vibqwv, kwvkmqdml qv tqjmzbg, ivl lmlqkibml bw bpm xzwxwaqbqwv bpib itt umv izm kzmibml mycit.

- How can we read such a message without knowing the key?

Brute Force Attack

encrypted message

Nwcz akwzm ivl amdmv gmiza iow wcz nibpmza jzwcopb nwzbp wv bpqa kwvbqvmvb, i vme vibqwv, kwvkmqdml qv tqjmzbg, ivl lmlqkibml bw bpm xzwxwaqbqwv bpib itt umv izm kzmibml mycit.

- Brute force attack tries all 26 possible keys (k=0...25)
- One of them will yield a readable message
- Rest will still look encrypted

Frequency Analysis

- We know that *e* is the most common letter in English
- Count which is the most common letter in the message
- That's probably the letter *e* in the original

Frequency Analysis Example

- There's 18 occurences of the letter *m*

encrypted message

Nwcz akwz**m** ivl a**m**d**m**v g**m**iza iow wcz nibp**m**za jzwcopb nwzbp wv bpqa kwvbqv**m**vb, i v**m**e vibqwv, kwvk**m**qd**m**l qv tqj**m**zbg, ivl l**m**lqkib**m**l bw bp**m** xzwxwaqbqwv bpib itt u**m**v iz**m** kz**m**ib**m**l **m**ycit.

Let $y = ord(m) = 12$, $x = ord(e) = 4$, and remember:

$$x = (y - k) \, (mod \, n)$$

$$4 = (12 - k)$$

$$k = (12 - 4) = 8$$

Frequency Analysis Solution

encrypted message

```
Nwcz akwzm ivl amdmv gmiza iow wcz nibpmza jzwcopb nwzbp wv bpqa
kwvbqvmvb, i vme vibqwv, kwvkmqdml qv Tqjmzbg, ivl lmlqkibml bw bpm
xzwxwaqbqwv bpib itt umv izm kzmibml mycit.
```

decrypted message

```
Four score and seven years ago our fathers brought forth on this
continent, a new nation, conceived in Liberty, and dedicated to the
proposition that all men are created equal.
```

How Do We Improve the Cipher?

- How do we improve this cipher?
- First, we need to identify the problems.
- What was the problem with brute force?

How Do We Improve the Cipher?

- How do we improve this cipher?
- First, we need to identify the problems.
- What was the problem with brute force?

How Do We Improve the Cipher?

- How do we improve this cipher?
- First, we need to identify the problems.
- What was the problem with brute force?

Substitution Cipher

- A *substitution cipher* maps from one alphabet to another
- Can map from and to same alphabet, but scrambled

substitution table

plaintext	ABCDEFGHIJKLMNOPQRSTUVWXYZ
ciphertext	THEQUICKBROWNFXJMPDVRLAZYG

One-to-One Functions

- This is known as a *one-to-one function*, or a *mapping*, or *permutation*
- Maps one input letter to exactly one output letter
- And vice-versa

Does This Solve Our Problem?

- Caesar cipher had only 26 possible keys
- How many does a substitution cipher have?

How Many Ways to Scramble 26 Letters?

- First letter may map to any of the 26 letters
- Second letter may map to 25 remaining letters
- Third letter may map to any of 24 remaining
- Do you see a pattern?

It's a Factorial!

$$26 \star (25 \star (24 \ldots)) = 26!$$

$$26! = 403291461126605635584000000$$

That's how many possible mappings there are

so obviously that's too many for brute-force attack

It's a Factorial!

$$26 \star (25 \star (24...)) = 26!$$

$$26! = 403291461126605635584000000$$

That's how many possible mappings there are

so obviously that's too many for brute-force attack