

Naval Academy Summer Seminar

Secret Sharing and Cryptography

Professor Will Traves

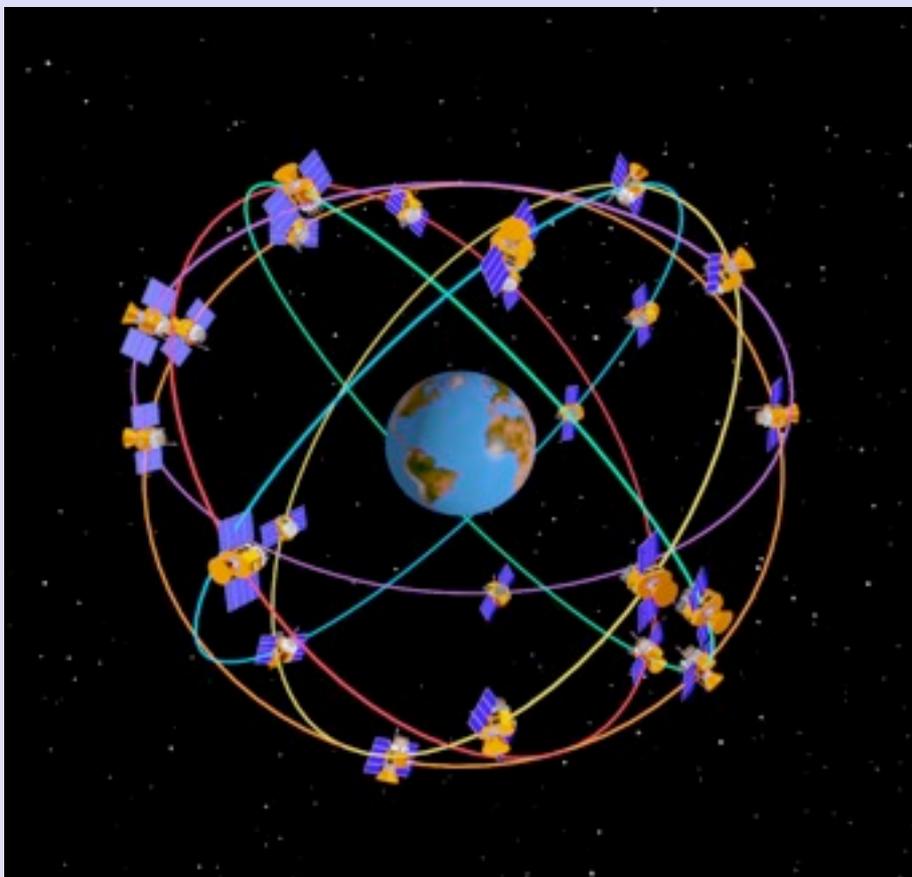
June 20, 2011

Math Courses at USNA

- All midshipmen take at least 4 math courses.
- It is possible to validate courses and get advanced placement (4 or 5 on AB/BC)
- Typical Placements:
 - 5% Precalculus
 - 66% Calculus I
 - 20% Calculus II
 - 8% Calculus III
 - 1% Higher Placements

Math Research

- The math department has over 60 faculty conducting research and teaching.



Some topics:

- Operations Analysis
- Cryptography
- Geometry
- Number Theory
- Computational Math
- Mathematical Physics
- GPS

Math Research

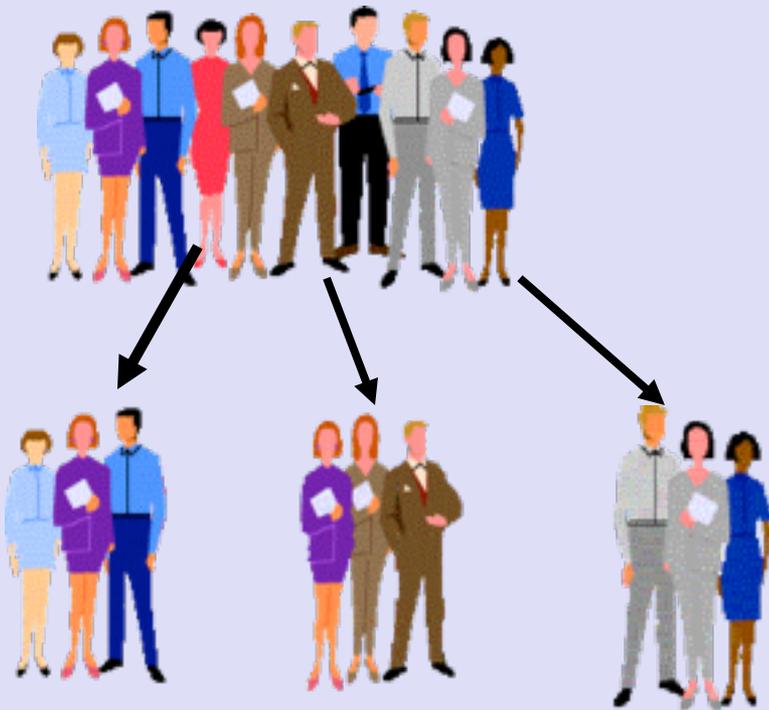
- **Math is interesting in its own right, but it is also an excellent preparation for studies in physics, economics and computer science.**
- **Midshipmen can become mathematics majors in one of two tracks, including an applied track. We also offer a quantitative economics major and an operations research major.**
- **Some math majors take the **honors** program. Others have done **Bowman** or **Trident** projects. All of these involve seniors doing directed research.**

Secret Sharing and Cryptography

- 1. Sharing a secret among several friends**
[Lagrange interpolation]
- 2. Sending secrets along insecure routes**
[Cryptographic protocols, modular arithmetic]
- 3. Breaking secret communications**
[Factoring large numbers]
- 4. Coin flipping over the telephone**
[Number theory]

Secret Sharing

We want to put some sensitive documents in a safe. The safe has a five digit combination. Ten people are authorized to view the documents, but only if two others agree. How can we allow groups of three people access to the combination so that no group of two gets any information about the combination?



Secret Sharing: Mathematics

Suppose we want to hide the code 54128 among ten people so that any three of them can recover the code. We pick a polynomial

$$P(x) = 54128 + 722x + 127x^2$$

so that the constant term $P(0)$ is our code. We then give the numbers $P(1), \dots, P(10)$ out to the ten people, one to each person.

Knowing 3 points on the parabola $y = P(x)$ should be enough to determine the curve – and the combination $P(0)$ – but this is trickier than you might think. The key is to use an idea called Lagrange interpolation.

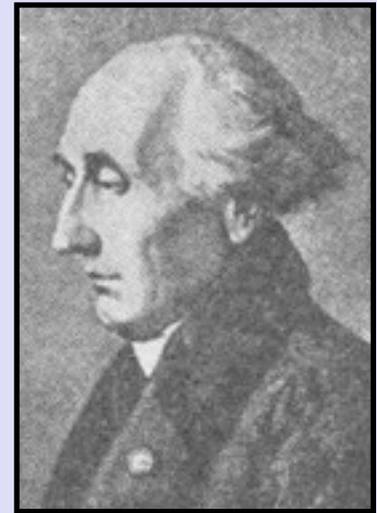
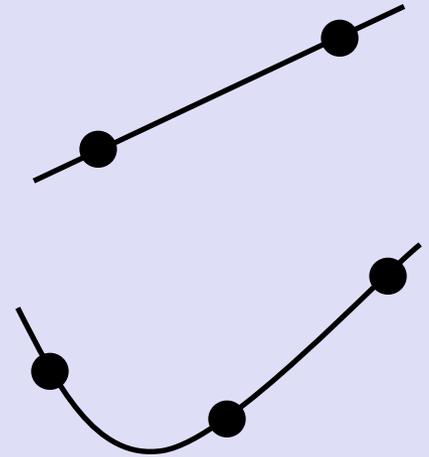
Lagrange Interpolation

Given two points, there is a unique line through both points.

Given three points, there is a unique parabola through all three.

In general, given D points, there is a unique polynomial function of degree $D-1$ passing through all of them.

Idea: $P(x) = a_0 + a_1x + \dots + a_{D-1}x^{D-1}$ has D coefficients so D data points suffice to determine the polynomial.



J. L. Lagrange
(1736-1813)

Lagrange Interpolation

To illustrate the idea, suppose that persons 1, 3 and 8 get together and share their secret data $P(1) = 54977$, $P(3) = 57437$, $P(8) = 68032$. This gives three points on the parabola: $A(1,54977)$, $B(3,57437)$ and $C(8,68032)$.

For each point, we find a degree 2 polynomial that is equal to 1 at the point and equal to 0 at the two other points.

For example: $P_A(x) = (x-3)(x-8)/(1-3)(1-8)$.

Then $54977 * P_A(x) + 57437 * P_B(x) + 68032 * P_C(x)$

is a degree two polynomial that agrees with the secret polynomial $P(x)$ at three points: A, B and C. Since both are degree 2, they must be equal. So the secret code is

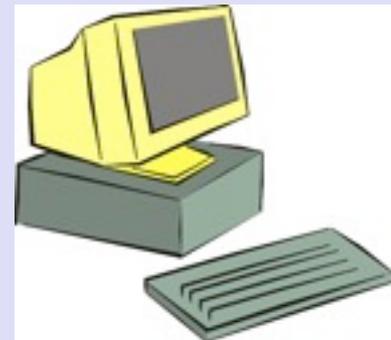
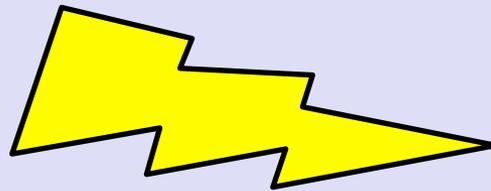
$54977 * P_A(0) + 57437 * P_B(0) + 68032 * P_C(0) = 54128$.

Sending Secrets: Cryptography

Motivation:

Military: Important to hide sensitive information from enemies and to read enemy communications.

Commercial: Wish to facilitate the secure transfer of data in order to encourage e-commerce.



Ciphers

**Caesar cipher: shift letters in a circular cycle (A to D, B to E, etc)
-- easy to use but simple to decode**



**Jefferson's Cipher Wheel
(perhaps from a European
"Black Chamber")**

**Substitution cipher: permute the letters in a set manner
(A to D, B to G, etc.)
-- many more codes are possible: how many?**

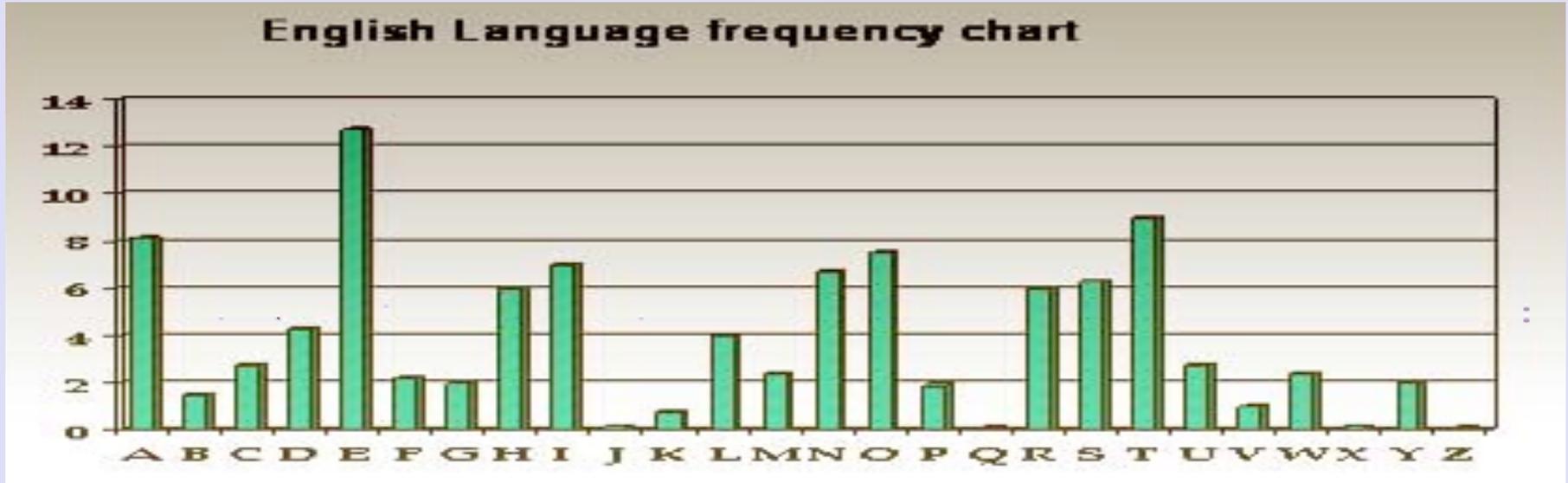
Substitution Challenge

The text has been encrypted using a substitution cipher. Is there any way to break the code and read the message?

**KSXNEQTCXXZOPLSXWTZBCXLPOITLLATBSERNAANEQAZ
WCDBOYCXWNECKCEQBXL SOFCQNICA ILEWBOWTBWXNBOWL
KNOILJBXRTLTCOPLXIBKTNFWLILFYBWBCEKRTZNEWTB
FNKKABLPWTBGLLDTCXXZOWXSQQABORNWTWTBOBYXLGABFO
NEKBCANEQRNWTWTBFTBEBBKOWLJNLACWBOLFBOITLLAXSABO**



Frequency Analysis



ake a wsh → ?

ay hee e → ?

app i tha → ?

B appears most often → **B** is probably **e**

TB appears a lot, but **BT** never → **T** is probably **h**

WTB appears the most of all **_TB** words → **W** is probably **t**

RNth appears several times → perhaps **RN** is **wi**

NE is **iE** and appears often → **E** is probably **n**

KSXinQhCXXZOPLSXthZeCXLPOIhLLAheSnwiAAinQAZ
tCDeOYCXtinCKCnQeXLSOFCQiICA ILnteOthetXieOtL
KiOILJeXwhLhCOPLXieKhiFtLILFYeteCnKwhZinthe
FiKKAeLPtheGLLDhCXXZOtXSQQAeOwiththeOeYXLGAeFO
inKeCAinQwiththeFheneeKOtLJiLACteOLFeOIhLLAXSAeO

with theF he → ?

inQ with the → ?

he neeKO → ?

B appears most often → **B** is probably **e**

TB appears a lot, but **BT** never → **T** is probably **h**

WTB appears the most of all **_TB** words → **W** is probably **t**

RNth appears several times → perhaps **RN** is **wi**

NE is **iE** and appears often → **E** is probably **n**

KSXinQhCXXZOPLSXthZeCXLPOIhLLAheSnwiAAinQAZ
tCDeOYCXtinCKCnQeXLSOFCQiICA ILnteOthetXieOtL
KiOILJeXwhLhCOPLXieKhiFtLILFYeteCnKwhZinthe
FiKKAeLPtheGLLDhCXXZOtXSQQAeOwiththeOeYXLGAeFO
inKeCAinQwiththeFheneeKOtLJiLACteOLFeOIhLLAXSAeO

with theF he → ?

he needs tL → ?

inQ with the → ?

[Go to WORD]

he neeKO → ?

**dSXinghCXXZsPoSXthZeCXoPsIhooAheSnwiAAingAZ
tCDesYCXtinCdCngeXoSsmCgilCAIontesthetXiesto
disIoJeXwhohCsPoXIedhimtoIomYeteCndwhZinthe
middAeoPtheGooDhCXXZstXSggAeswiththeseYXoGAems
indeCAingwiththemheneedstoJioACtesomesIhooAXSAes**

**dSXinghCXXZsPoSXthZeCXoPsIhooAheSnwiAAingAZ
tCDesYCXtinCdCngeXoSsmCgiICAiontesthetXiesto
disIoJeXwhohCsPoXIedhimtoIomYeteCndwhZinthe
middAeoPtheGooDhCXXZstXSggAeswiththeseYXoGAems
indeCAingwiththemheneedstoJioACtesomesIhooAXSAes**

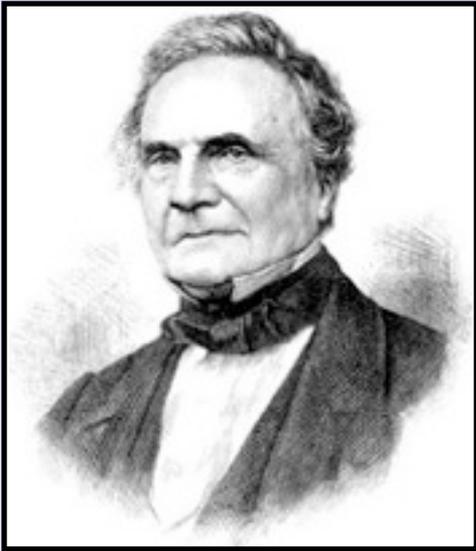


During Harry's fourth year of school he unwillingly takes part in a dangerous magical contest. He tries to discover who has forced him to compete and why. In the middle of the book Harry struggles with these problems. In dealing with them he needs to violate some school rules.



Advanced Ciphers

Vigenère Cipher: consists of multiple Caesar ciphers based off a key



Charles Babbage

-- eg. the key **ABE** transforms
THE HAWK TRAVELS AT DAWN to
UJI ICBL VVBXIMU BV HBYS

-- look for period and use frequency analysis:
If the same set of letters appears twice in
a long text, then it is likely that the length of the
key divides the displacement of the reoccurring
word.

Once the key length is determined, you can
use frequency analysis to determine each letter.

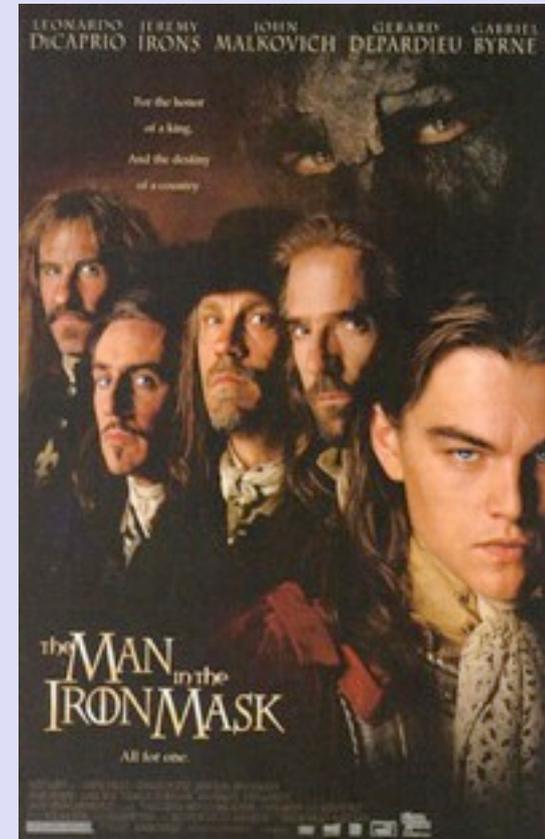
The Man in the Iron Mask

Louis XIV imprisoned a mysterious stranger in the Savoy jail , allowing him to walk the battlements in an iron mask. Who was this masked man? Was he the king's twin?

Rossignol – Father and son team helped defeat the Huguenots in Realmont in 1626. They created the great cipher (unbroken for 200 years).

Bazeries – French military officer translates the cipher, guessing that it was a syllabic cipher (1893).

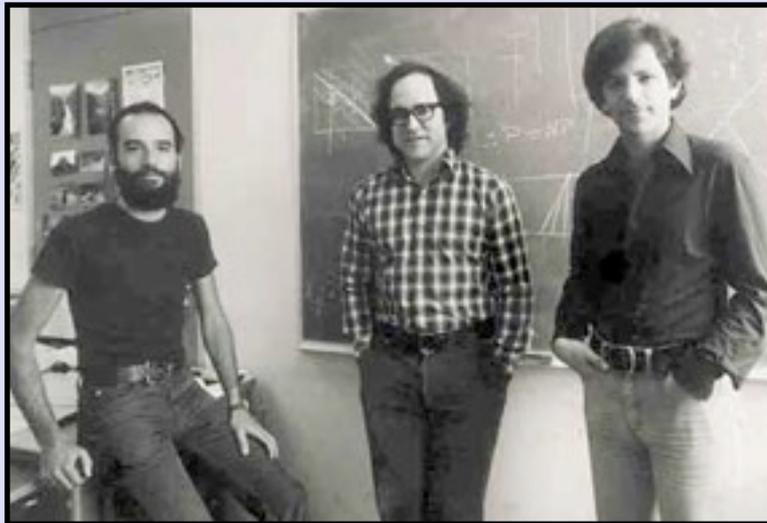
General Bulonde – Cowardice in Cuneo in the Piedmont campaign.



Modern Methods

Today we tend to avoid secret keys and the **key distribution** problem by using public key methods.

One of the most popular methods is the **RSA protocol**. This is based on modular arithmetic.



Rivest, Shamir and Adelman developed the RSA protocol on the outside. **Cocks and Williamson** had discovered it previously at GCHQ.

Modular Arithmetic



Think of **modular arithmetic** as “clock arithmetic”. We add and multiply numbers by only considering their remainders.

For instance, $3 \times 5 \bmod 12 = 15 \bmod 12 = 3 \bmod 12$
and $3 + 10 \bmod 12 = 1 \bmod 12$.

Modular arithmetic is simplest when our modulus is a prime. For example, 12 is not a prime and $3 \times 8 \bmod 12 = 0 \bmod 12$. Unfortunately, neither 3 nor 8 is $0 \bmod 12$.

Note: $x = y \bmod n$ means that n divides $x - y$.

Fermat's Little Theorem

If p is a prime, and a is a number relatively prime to p , then

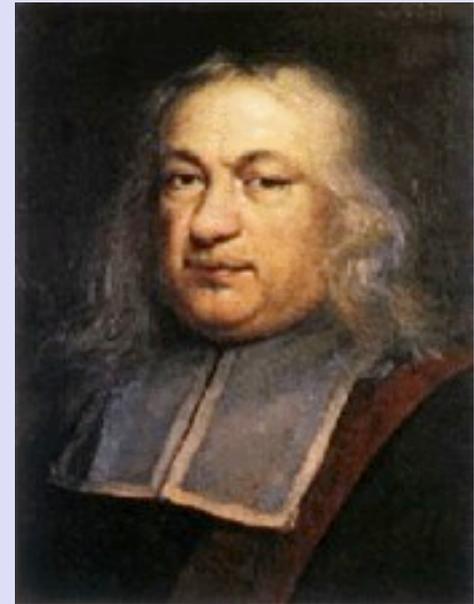
$$a^{p-1} = 1 \pmod{p}.$$

If p and q are primes, and $\Phi = (p-1)(q-1)$ and a is a number relatively prime to both p and q , then

$$a^{\Phi} = 1 \pmod{pq}.$$

Example: $p=3$, $q=5$, $a=2$.

Then $2^{2(4)} = 16^2 = 1 \pmod{15}$.



Pierre de Fermat

Fermat's Little Theorem

If p is a prime, and a is a number relatively prime to p , then

$$a^{p-1} = 1 \pmod{p}.$$

If p and q are primes, and $\Phi = (p-1)(q-1)$ and a is a number relatively prime to both p and q , then

$$a^{\Phi} = 1 \pmod{pq}.$$

Example: $p=3$, $q=5$, $a=2$.

Then $2^{2(4)} = 16^2 = 1 \pmod{15}$.

Fermat's Little Theorem

If p is a prime, and a is a number relatively prime to p , then

$$a^{p-1} = 1 \pmod{p}.$$

If p and q are primes, and $\Phi = (p-1)(q-1)$ and a is a number relatively prime to both p and q , then

$$a^{\Phi} = 1 \pmod{pq}.$$

Example: $p=3$, $q=5$, $a=2$.

Then $2^{2(4)} = 16^2 = 1 \pmod{15}$.

Fermat's Little Theorem

If p is a prime, and a is a number relatively prime to p , then

$$a^{p-1} = 1 \pmod{p}.$$

If p and q are primes, and $\Phi = (p-1)(q-1)$ and a is a number relatively prime to both p and q , then

$$a^{\Phi} = 1 \pmod{pq}.$$

Example: $p=3$, $q=5$, $a=2$.

Then $2^{2(4)} = 16^2 = 1 \pmod{15}$.



**Kayal, Saxena
and Agrawal used a
converse to FLT to
test for primality.**

RSA Cryptography

Alice wants to send a message to Bob without Eve discovering the message's content.

Bob first selects two large primes p and q . He keeps these secret and sends $n=pq$ to Alice. Eve might overhear n , but neither Eve nor Alice know p and q .

Bob also computes $\Phi=(p-1)(q-1)$ and picks an integer e relatively prime to Φ . He sends e to Alice and computes $d = 1/e \text{ mod } \Phi$.



RSA Cryptography

Alice takes her message and converts it to blocks of numbers $< n$.

To send a block m , she sends $E(m) = m^e \bmod n$.

Bob receives m^e and computes $D(m^e) = m^{ed} \bmod n$.

Now $e = 1/d \bmod \Phi$, so $ed = 1 + k\Phi$. But now

$$m^{ed} = m^{1+k\Phi} = m(m^\Phi)^k = m \bmod n$$

since $m^\Phi = 1 \bmod n$ by Fermat's Little Theorem.

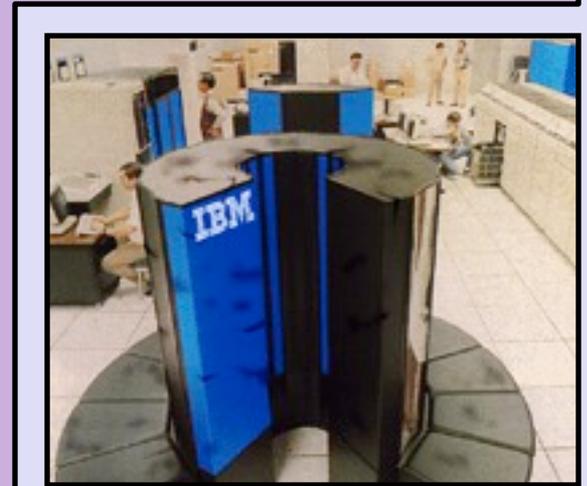
So Bob recovers Alice's original message!

Cracking RSA: Factoring

Eve needs to factor n to get Φ so she can get the decryption exponent d . Then she can recover the original message.

Difficult for large numbers:

- Fastest computer: 10^{12} divisions/sec
- Leads to about 10^{20} divisions/year
- so brute force attack on a 60 digit number will take about 10 billion years



Need better technology – mathematical technology

Factoring Challenges

Original Challenge: RSA-129, 1977
Solved in 1994: Atkins, Graff, Lenstra and Leyland
“The magic words are squeamish ossifrage”



A. Lenstra

RSA.com sponsors contests to factor integers

RSA-576 Prize: \$10,000 Decimal Digits: 174

RSA-640 Prize: \$20,000 Decimal Digits: 193

RSA-704 Prize: \$30,000 Decimal Digits: 212

...

RSA-2048 Prize: \$200,000 Decimal Digits: 617

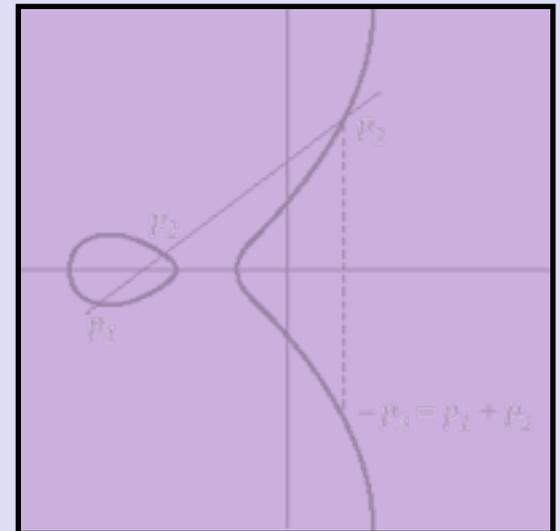
Advanced Factoring Methods

**Lenstra's Elliptic Curve Method –
Midn 1/c Privette, 2002.**

**(Quadratic) Sieve – If $n = pq$ then
the equation $a^2 = d$ has 4 solutions
mod n (rather than just two)!**

**So if $a^2 = b^2 \pmod n$ and a is not b or $-b \pmod n$, then
 $(a-b)(a+b) = 0 \pmod{pq}$ and so p must divide one of $a-b$ and
 q must divide the other.**

**To find p or q we just find the greatest common divisor of
 $n=pq$ and $a-b$.**



Euclidean GCD Algorithm

The Euclidean Algorithm gives a fast way to find the GCD of two numbers.

$$\text{GCD}(36,15) : \quad 36 = a \cdot 15 + r_1 \quad \text{with } r_1 < 15.$$

$$36 = 2(15) + 6.$$

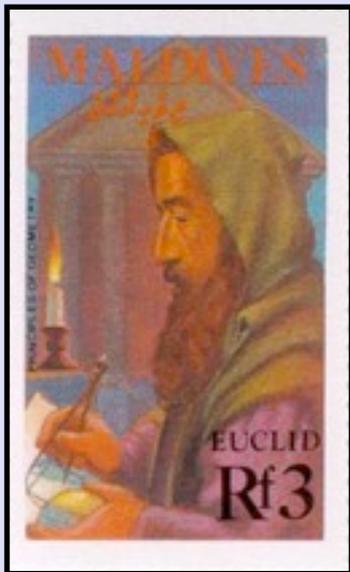
$$15 = b \cdot 6 + r_2 \quad \text{with } r_2 < 6.$$

$$15 = 2(6) + 3$$

$$6 = 2(3) + 0$$



GCD is 3.



Euclid on a Maldives Island stamp.

Steganography



Digital Invisible Ink Toolkit

Coin Flipping over the Phone

Can we safely flip coins over the telephone?

Alice and Bob inherit a car from their uncle. Since they live in different cities, they agree to flip for a coin for the car. Can they do it over the phone? Bob is willing to flip, but how can Alice ensure that the result is fair?

It may seem impossible, but they can do it if Alice and Bob know some number theory!



Square Roots Mod p

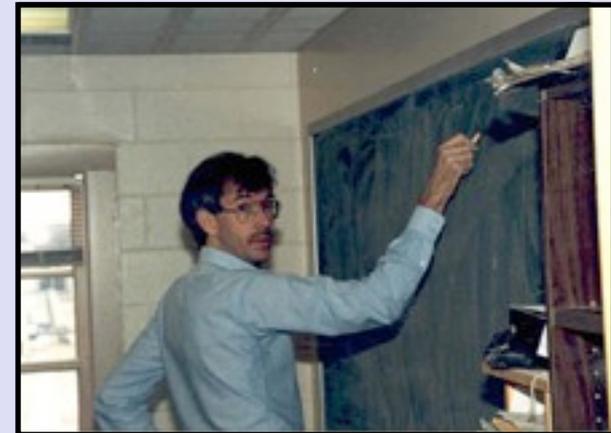
Suppose that $p \equiv 3 \pmod{4}$. Some numbers have a square root mod p , while others do not. In fact, y has a square root mod p if and only if $-y$ does not have square root mod p .

There is a simple formula for this root:

$$x = \pm y^{(p+1)/4} \pmod{p}.$$

Example: $p = 11$ and $y = 5$. Then

$$x = \pm 5^3 \pmod{11} = \pm 4 \pmod{11}.$$



L. Washington

Square Roots mod pq

Chinese Remainder Theorem: Solving $x^2 = d \pmod{pq}$ is essentially equivalent to solving $x^2 = d \pmod{p}$ and $x^2 = d \pmod{q}$.

Example: Solve $x^2 = 71 \pmod{77}$. First, $x^2 = 1 \pmod{7}$ and $x^2 = 5 \pmod{11}$. Solve using previous slide to find $x = \pm 1 \pmod{7}$ and $x = \pm 4 \pmod{11}$. We find interpolating values using Fermat's LT:

$$7^{10} = 0 \pmod{7}$$

$$1 \pmod{11}$$

$$11^6 = 1 \pmod{7}$$

$$0 \pmod{11}.$$


$$56 \pmod{77}$$


$$22 \pmod{77}$$

Now one solution is $x = 4(56) + 1(22) \pmod{77} = 15 \pmod{77}$. The others are -15 and ± 29 .

Coin Flipping

Principle: If we know p and q , we can find all solutions to $x^2 = y \pmod{pq}$. If we know two “different” solutions then we can find p and q .

ALICE

$p, q = 3 \pmod{4}$

$y = x^2$

solns: $x, -x,$
 $z, -z$

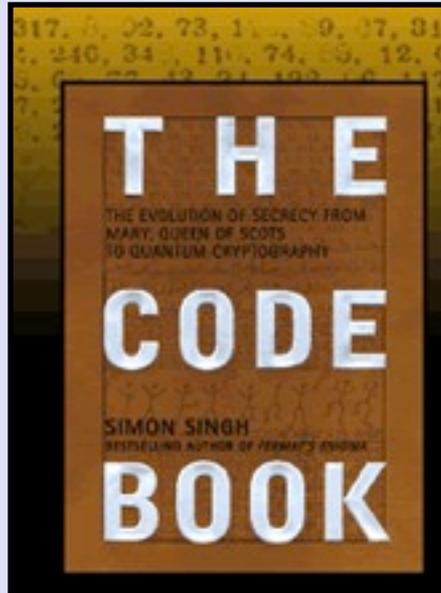
BOB

$n = pq$

x

$\pm z$: Bob Wins – provide p, q
to certify
 $\pm x$: Bob Loses – has no extra info.

Recommended Reading



The Code Book.
Simon Singh.

Cryptography and Coding Theory.
Wade Trappe and Lawrence C.
Washington.

