Public Key Cryptography

Discrete Mathematics

Evgeny Skvortsov

Previous Lecture

- Caesar cipher
- Chinese Remainder Theorem

Fermat's Theorem

- **Fermat's Great (Last) Theorem.**
  For any $n > 2$, the equation $x^n + y^n = z^n$ does not have integer solutions $x,y,z > 0$

- It had remained unproven for 358 years (posed in 1637, proved in 1995)

- Andrew Wiles proved it in 1995

Fermat's Little Theorem

- **Fermat's Little Theorem.**
  If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

- Clearly, it suffices to consider only residues modulo p.

Z_5

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Fermat's Little Theorem (cntd)

- Fermat's Little Theorem was improved by Euler
- **Fermat's Little Theorem improved**

  For any integers m and a such that they are relatively prime

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

  where $\varphi(m)$ denotes the Euler totient function, the number of numbers $0 < k < m$ relatively prime with m

- Example: Z_8

Public Key Cryptography

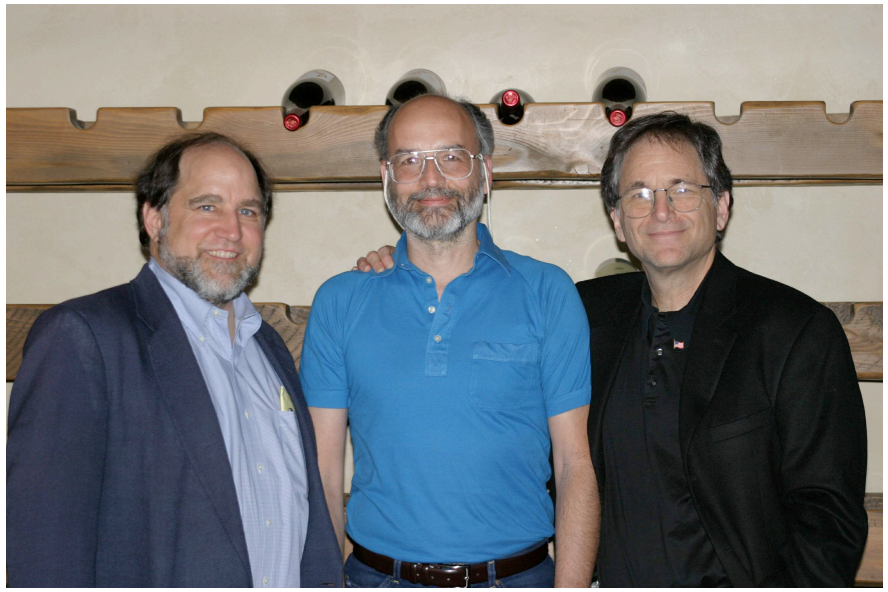
- Earlier we considered Caesar cipher. To encrypt and decrypt messages using this cipher one needs to know the key
- Caesar cipher uses the same key for encryption and decryption; it is secret, and if one knows the key he knows everything.
- Public key cryptosystems use a different approach
- Such a system uses different keys for encryption and decryption:

  Every person has a key for encryption, and can write an encrypted message

  But this does not help to decrypt the message

RSA Cryptosystem

- RSA stands for the names of the inventors: Rivest, Shamir, Adleman



From left to right:
Ron Rivest
Adi Shamir
Len Adleman

- RSA key: a modulus $n = pq$, where p and q are large prime numbers (current standards are 128, 256, or 512 digits each), n is public while p and q are secret, and

  an exponent e relatively prime with $(p – 1)(q – 1)$

RSA Encryption

- In the RSA method, messages are translated into an integer (a short message) or a sequence of integers
- Let M be the plaintext (the original message). Then the ciphertext is the residue

$$C \equiv M^e \pmod{n}$$

- Example. Encrypt the message STOP using the RSA cryptosystem with $p = 43$ and $q = 59$, so that $n = 43 \cdot 59 = 2537$, and with $e = 13$.

  Note that $\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$
- Solution. Translate the letters of STOP into their numerical equivalents and group them into groups of four: 1819 1415

  Encrypt them using $C \equiv M^{13} \pmod{2537}$. We get

  $1819^{13} \equiv 2081 \pmod{2537}$ and $1415^{13} \equiv 2182 \pmod{2537}$

  Thus, the encrypted message is 2081 2182

RSA Decryption

- The decryption key d is the inverse of e modulo $(p-1)(q-1)$. It is secret!

  Since $\gcd(e, (p-1)(q-1)) = 1$, the inverse exists.

- Indeed, $de \equiv 1 \pmod{(p-1)(q-1)}$, therefore there is k such that $de = 1 + k(p-1)(q-1)$. Hence

$$C^d \equiv (M^e)^d \equiv M^{de} \equiv M^{1+k(p-1)(q-1)} \pmod{n}$$

Note that $\varphi(n) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) = (p-1)(q-1)$

By Fermat's Little Theorem, $M^{k(p-1)(q-1)} = (M^{\varphi(n)})^k \equiv 1 \pmod{n}$

Hence, $C^d \equiv M \times M^{k(p-1)(q-1)} \equiv M \pmod{n}$

Thus $C^d \equiv M \pmod{n}$

Example

- We receive the encrypted message 0981 0461. What is the plaintext if it was encrypted using the RSA cipher fro the previous example.
- Solution

  The encryption keys were $n = 43 \cdot 59$ and $e = 13$.

  It is not hard to see that $d = 937$ is the inverse of 13 modulo $42 \cdot 58 = 2436$.

  Therefore to decrypt a cipher block C, we compute

$$P \equiv C^{937} \pmod{n}$$

  In our case we have

  $0981^{937} \equiv 0704 \pmod{2537}$ and $0461^{937} \equiv 1115 \pmod{2537}$

  Thus the plaintext is 0704 1115, that is HELP

Why RSA Works

- The secrecy comes from the fact that it is incredibly difficult to find an inverse modulo a big number if we do not know its prime decomposition.
- However, it is also very difficult to find a prime decomposition of a number if its prime factors are big. The most efficient factorization method known requires billions of years of work of the fastest computers to factorize a 400-digit number.

- We need n to be the product of 2 prime numbers, because the method works only if the message is relatively prime with n. Thus n needs to have very few divisors.

A note. There was a repeating mistake at the midterm. So I would like to emphasize:

COUNTABLE IS NOT FINITE