Modern Cryptography

Daryl DeFord and David Freund

Dartmouth College
Department of Mathematics

Johns Hopkins University - Center for Talented Youth
Science and Technology Series
National Cyber Security Awareness Month

Dartmouth

Abstract

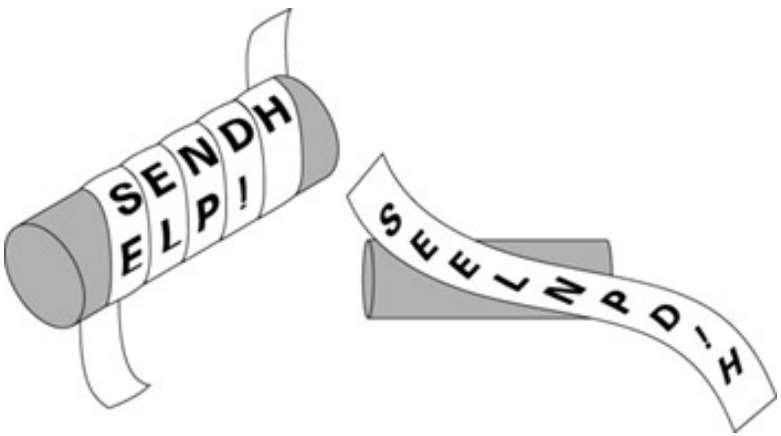
Abstract

From the simple substitution methods of the ancient Greeks to today's computerized elliptic curve algorithms, various codes and ciphers have been used by both individuals and governments to send secure messages. As an increasing amount of our personal communications and data have moved online, understanding the underlying ideas of internet security has become increasingly important. In this workshop we will present the mathematical basis of public-key cryptography; providing hands-on experience with some of the most common encryption algorithms that are used on the internet today.

Outline

What is cryptography?

- Study of secret writing
- A means of protecting or hiding information
- Techniques for analyzing encoding and decoding processes



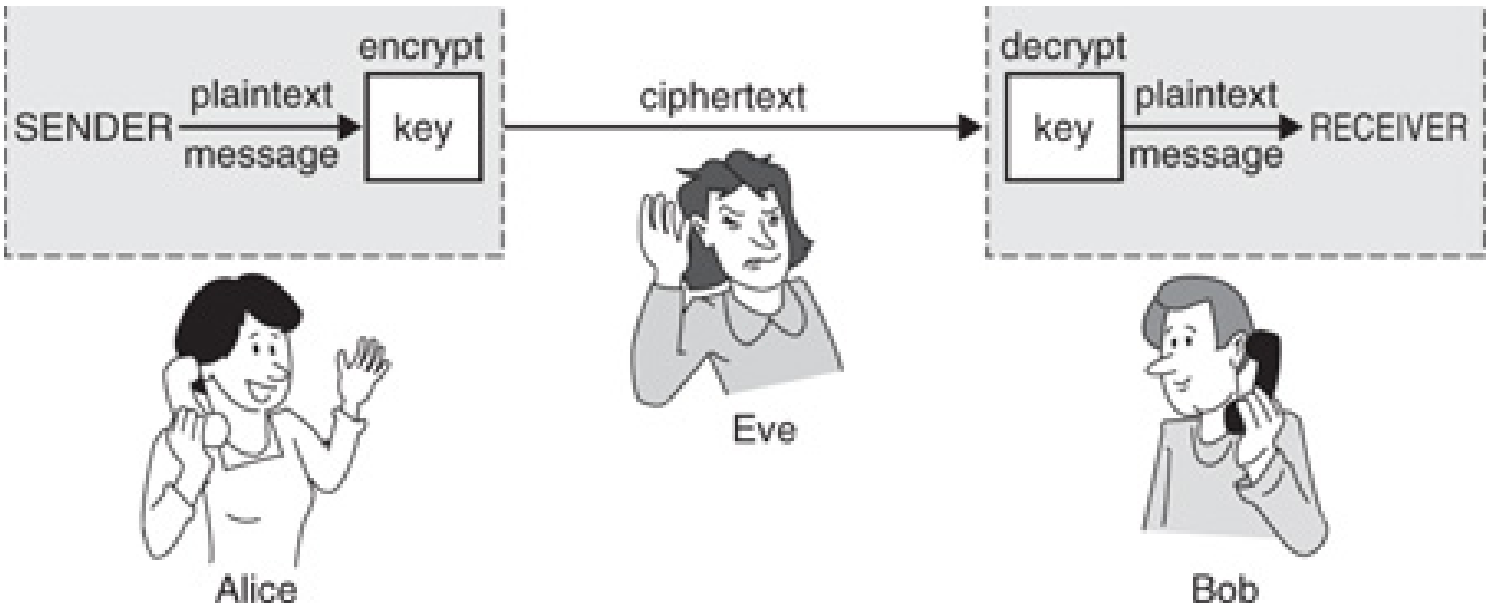
http://flylib.com/books/2/827/1/html/2/images/1004.jpg

Basic Definitions

- Plaintext
- Ciphertext
- Encryption
- Decryption
- Keys
- Cryptanalysis

Standard Setup

- Alice wants to send a message to Bob
- Eve, a cryptanalyst, wants to intercept/decode the message:



http://tools.rosinstrument.com/pb/m/12317.htm

Symmetric Cryptography

- A single key for both encryption and decryption
- Initialization must be done privately
- Not reusable

Caesar Cipher

- Simple substitution cipher
- Broken about 800 A.D.
- Vigenère ciphers

Activity 1: Caesar Ciphers

This cipher disk was used in the American Civil War.

texttttthttp://ciphermachines.com/

Public–Key Cryptography

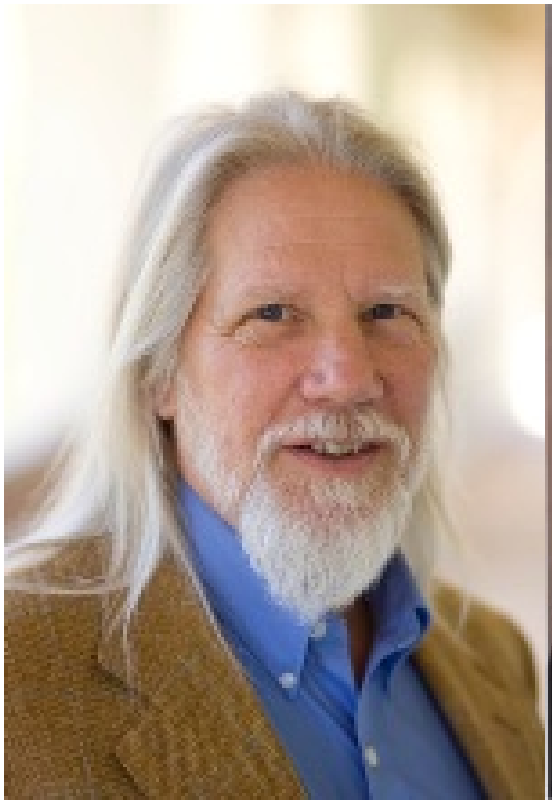
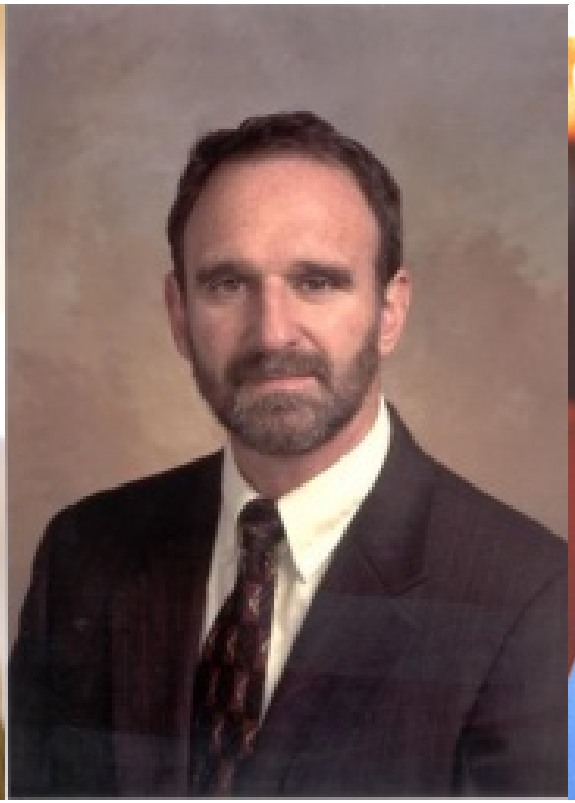
Public–Key Cryptography

Asymmetric Cryptography

- Problems with symmetric cryptosystems:
  - Transmitting the key
  - Number of keys needed
- Computational feasibility
- Asymmetric functions
- What does security mean?

History

- Whitfield Diffie, Martin Hellman, and Ralph Merkle

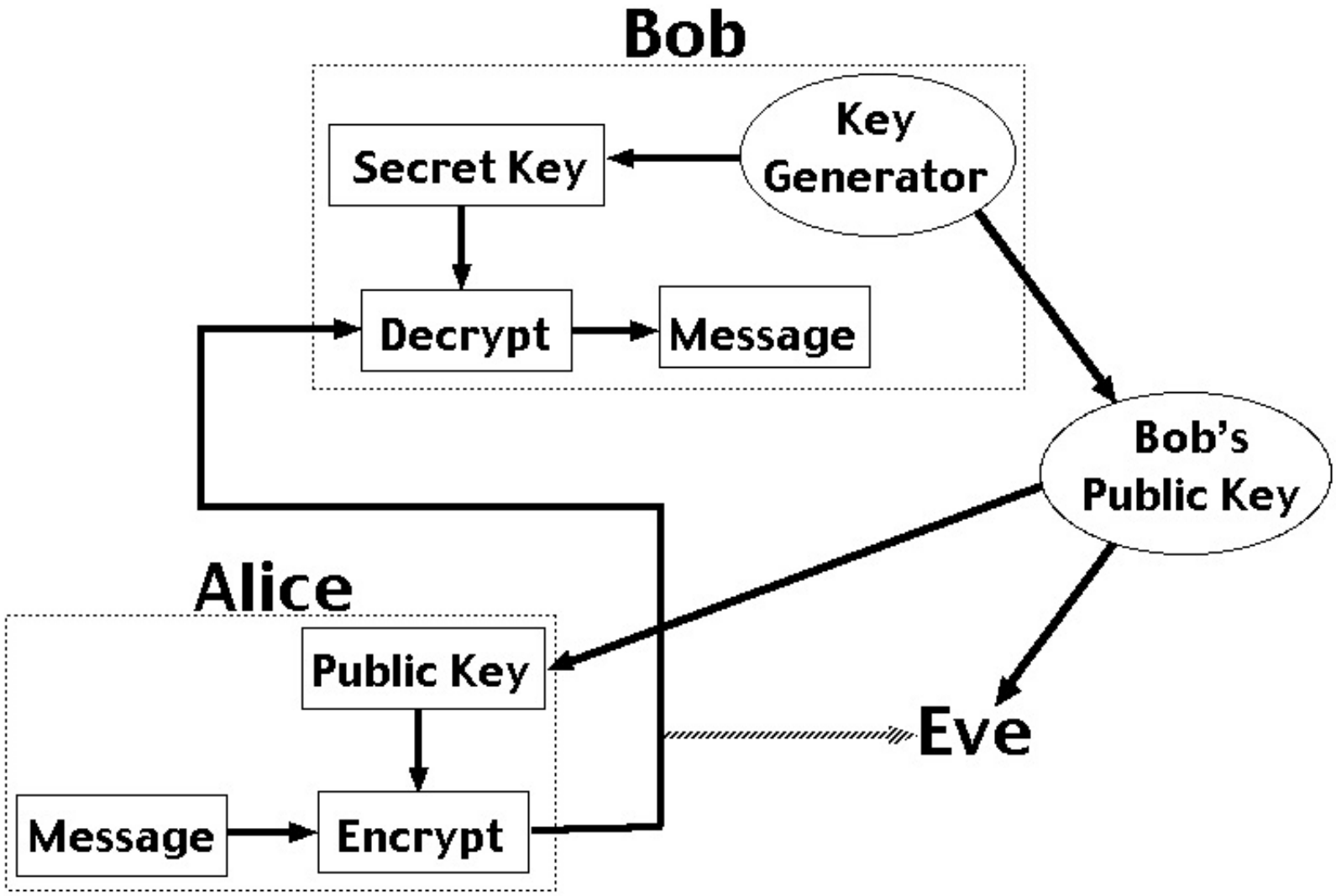




http://www.cryptomathic.com/news-events/events/barclays-csg-event/speakers
http://www.ieeeghn.org/wiki/index.php/Oral-History:Martin_Hellman
http://www.foresight.org/Updates/Update43/Update43.4.html

"Key" Ideas

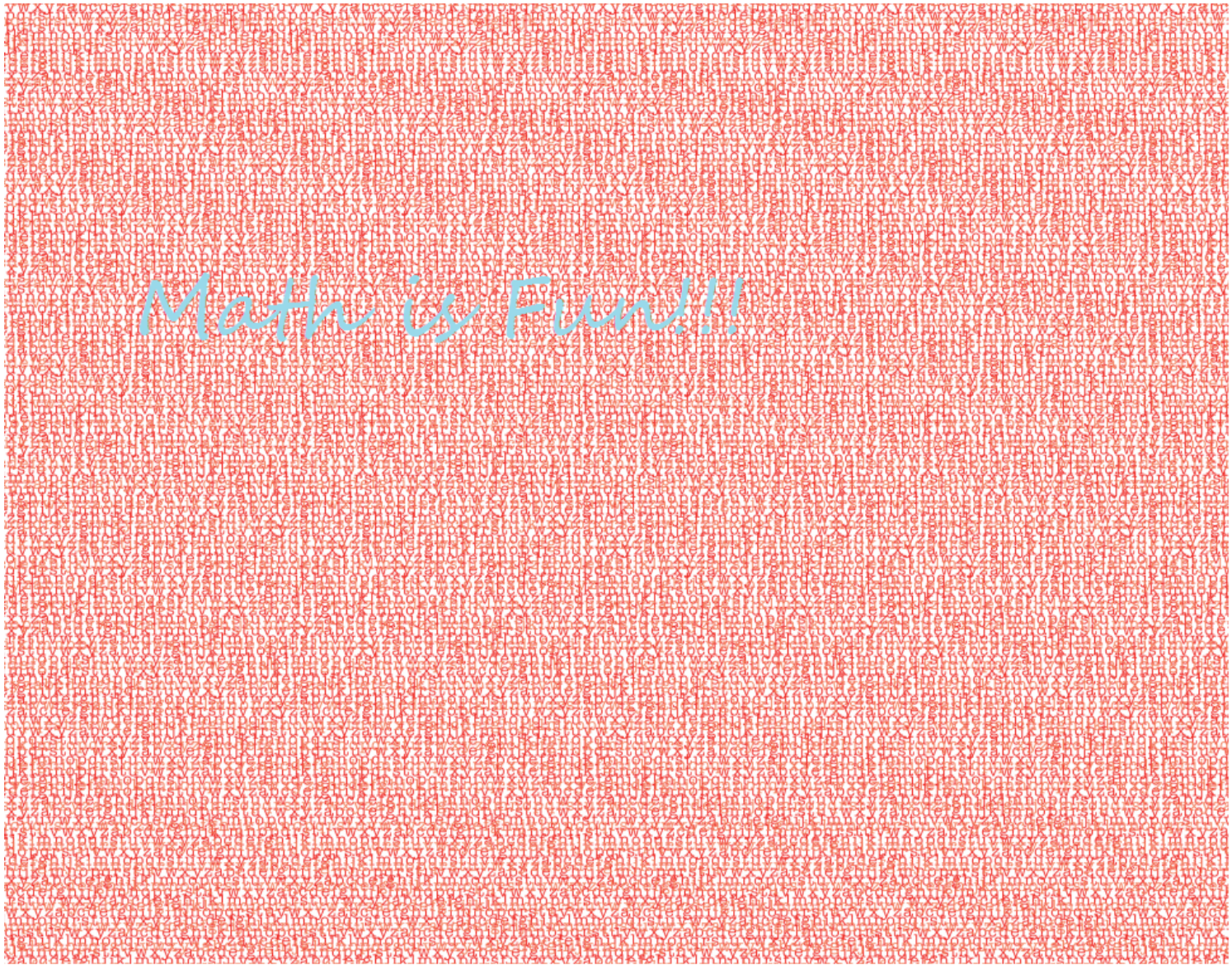
- Sending secure messages
  - Every individual generates a public and private key
  - Alice encrypts her message using Bob's public key and sends the ciphertext to Bob
  - Bob recovers the plaintext from the ciphertext by using his public key.
- Authenticating messages (requires symmetric functions)
  - Alice signs her message by encrypting it with her private key
  - Bob uses Alice's public key to verify that Alice sent the message.

Example 2



http://pajhome.org.uk/crypt/rsa/intro.html

Activity 2: Public–Key Cryptography



Number Theory

Number Theory

Mathematical Preliminaries

- Fundamental Theorem of Arithemtic
- Examples:
  - $15 = 3 \cdot 5$
  - $24 = 2^3 \cdot 3$
  - $101 = 101$
- Greatest Common Divisor
- Examples:
  - $(6, 10) = 2$
  - $(12, 63) = 3$
  - $(9, 17) = 1$

Euler φ

- Counts the number of $k < n$ such that $(k, n) = 1$.
- $$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$
- Examples:
  - $\varphi(12) = 4 \qquad \{1, 5, 7, 11\}$
  - $\varphi(7) = 6 \qquad \{1, 2, 3, 4, 5, 6\}$
  - $\varphi(20) = 8 \qquad \{1, 3, 7, 9, 11, 13, 17, 19\}$

Modular Arithmetic

- Clocks

http://cdn.lssproducts.com/images/uploads/101036_Clock.jpg

- Standard system of residues

Modular Examples

- $123 \equiv 3 \pmod{10}$
- $287569832 \equiv 2 \pmod{10}$
- $5 \equiv 1 \pmod{4}$
- $33 \equiv 1 \pmod{4}$
- $-1 \equiv 3 \pmod{4}$
- $8 \equiv 0 \pmod{4}$
- $4 \equiv 0 \pmod{4}$

Modular Inverses

- Standard arithmetic operations $+, -, \cdot$
- Problems with division: $2x \equiv 1 \pmod 7$ vs $2x \equiv 1 \pmod 6$
- When do inverses exist?

Fermat's Little Theorem

Theorem (Fermat)

Let a and n be any integers such that $(a, n) = 1$. Then

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

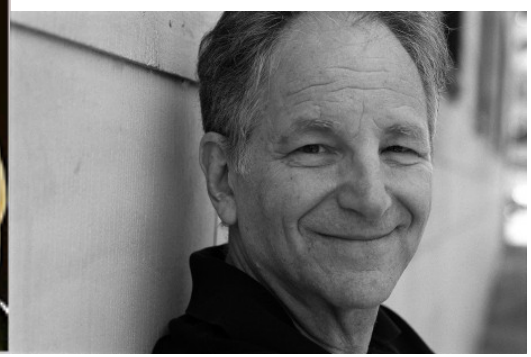
Algorithms

Algorithms

History

- Ron Rivest, Adi Shamir, and Leonard Adleman





http://people.csail.mit.edu/rivest/
http://www.nytimes.com/2007/11/17/technology/17code.html?_r=0
http://www.heidelberg-laureate-forum.org/blog/laureate/leonard-max-adleman/

Key Generation

- Select two large primes p and q
- Compute $\varphi(pq) = (p-1)(q-1)$
- Choose some integer r such that $(r, \varphi(pq)) = 1$
- Comptue x such that $rx \equiv 1 \pmod{\varphi(pq)}$
- Public Key:
  - pq
  - r
- Private Key:
  - p
  - q
  - $\varphi(pq)$
  - x

RSA Algorithm

- Alice wants to send a message to Bob
- Alice takes her message M and computes $C = M^r \pmod{pq}$
- Alice sends C to Bob
- Bob computes.

$$C^x = (M^r)^x = M^{rx} = M^{k\varphi(pq)+1} = (M^{\varphi(pq)})^k M = 1^k M = M \pmod{pq}$$

RSA Example (Bob's Key Generation)

- Select $p = 11$ and $q = 23$
- We first compute $\varphi(253) = 220$
- Next, we choose $r = 13$ and compute $x = 17$ since $13 \cdot 17 = 221 \equiv (\mathrm{mod}\ 220)$
- Bob releases the public key: $(253, 13)$
- Bob keeps the private key secret: $(11, 23, \varphi(253), 17)$.

RSA Example (Alice Encodes Her Message)

- Alice chooses a message, $M = 18$.
- She uses Bob's public key to encrypt the message by computing $M^r \pmod{pq}$

$$18^{13} = 2082296486567116 8 \equiv 2 \pmod{253}$$

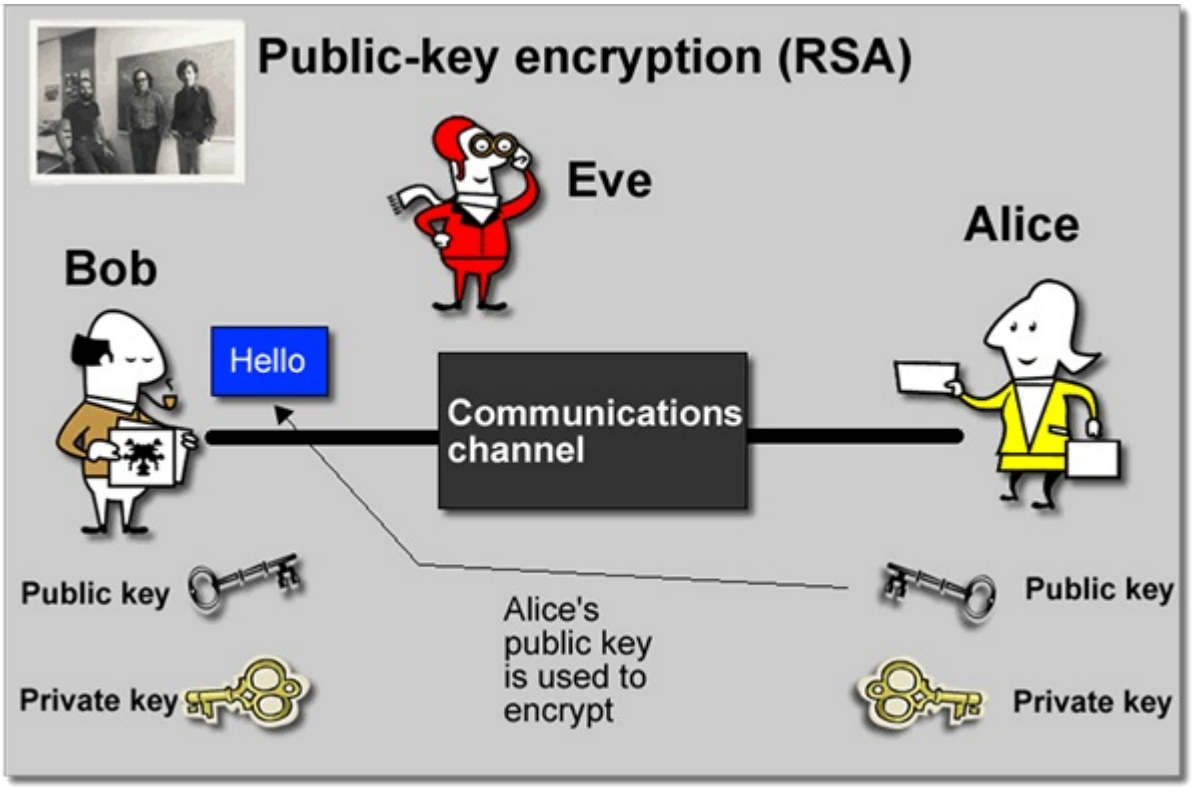
- Alice sends the ciphertext $C = 2$ to Bob.

RSA Example (Bob Decodes The Message)

- In order to decode C, Bob uses his private key:

$$2^{17} = 131072 \equiv 18 = M \pmod{253}$$

Activity 3



http://www.itportal.in/2011/11/rsa-algorithm-information-security-be.html

Discrete Log

- Relies on the difficulty of solving $a^x \equiv b \pmod{n}$.
- Diffie–Hellman–Merkle
- El Gamal
- Efficient quantum algorithm

Elliptic Curves

- An elliptic curve is the set of solutions (x, y) to an equation of the form $y^2 = x^3 + AX + B$.
- 'Addition' operation on points with rational coordinates
- Computations are difficult so key sizes are much smaller
- Efficient quantum algorithm

Knapsack Codes

- Merkle–Hellman
- Subset sum problem
- NP–Complete
- Recent Research

Thanks to ...

- Dartmouth College Department of Mathematics
- Johns Hopkins University– Center for Talented Youth

Further Reading

- Applied Cryptography (Schneier[1])
- Cryptography: A Very Short Introduction (Piper and Murphy)
- Cryptography and Data Security (Denning)
- Cryptanalysis of Number Theoretic Ciphers (Wagstaff)

[1] Anything by Schneier is worth reading

Questions

Questions???

THANK YOU!!!