Cryptography: An Art and Science

Sujit Prakash Gujar

sujit@csa.iisc.ernet.in
Indian Institute of Science, Bangalore-12

September 15, 2007.

Agenda

- Motivation

Agenda

- Motivation
- Objectives of Cryptography.

Agenda

- Motivation
- Objectives of Cryptography.
- Evolution: Need for Mathematical tools in cryptography.

Agenda

- Motivation
- Objectives of Cryptography.
- Evolution: Need for Mathematical tools in cryptography.
- Encryption/Decryption: Art and Science.

Agenda

- Motivation
- Objectives of Cryptography.
- Evolution: Need for Mathematical tools in cryptography.
- Encryption/Decryption: Art and Science.
- Hard Problems.

Agenda

- Motivation
- Objectives of Cryptography.
- Evolution: Need for Mathematical tools in cryptography.
- Encryption/Decryption: Art and Science.
- Hard Problems.
- RSA: Integer Factorization.

Agenda

- Motivation
- Objectives of Cryptography.
- Evolution: Need for Mathematical tools in cryptography.
- Encryption/Decryption: Art and Science.
- Hard Problems.
- RSA: Integer Factorization.
- Conclusions.

Motivation

- Colonel wants to convey some military plan of action to Lieutenant Colonel.

Motivation

- Colonel wants to convey some military plan of action to Lieutenant Colonel.
- World War I: Zimmermann Telegram.

Motivation

- Colonel wants to convey some military plan of action to Lieutenant Colonel.
- World War I: Zimmermann Telegram.
- World War II:Famous for cipher breaking.

Motivation

- Colonel wants to convey some military plan of action to Lieutenant Colonel.
- World War I: Zimmermann Telegram.
- World War II:Famous for cipher breaking.
- On-line banking.

Objectives of Cryptography

- Privacy: Ciphers
- Authentication: Digital Signatures.
- Data Integrity: Message Digest
- Non-repudiation: Digital Signatures.

Evolution of Cryptography

- Steganography: art and science of writing hidden messages.

Evolution of Cryptography

- Steganography: art and science of writing hidden messages.
- Demeratus: Wooden Tablet. (440 BC)

Evolution of Cryptography

- Steganography: art and science of writing hidden messages.
- Demeratus: Wooden Tablet. (440 BC)
- Substitution Ciphers.

Evolution of Cryptography

- Steganography: art and science of writing hidden messages.
- Demeratus: Wooden Tablet. (440 BC)
- Substitution Ciphers.
- Statistical Analysis.

Evolution of Cryptography
Polyalphabetic substitution

- Vigenere cipher: polyalphabetic substitution.

Evolution of Cryptography
Polyalphabetic substitution

- Vigenere cipher: polyalphabetic substitution.
- Enigma.

Evolution of Cryptography
Polyalphabetic substitution

- Vigenere cipher: polyalphabetic substitution.
- Enigma.

Evolution of Cryptography

- Use of Keys.
- Secret Algorithms vs. Secret Key Algorithms.
- Distribution of keys?

Evolution of Cryptography

- Use of Keys.
- Secret Algorithms vs. Secret Key Algorithms.
- Distribution of keys?

Evolution of Cryptography

- Use of Keys.
- Secret Algorithms vs. Secret Key Algorithms.
- Distribution of keys?

Cipher: Art and Science

- Cipher: an encryption and decryption algorithm.
- Encryption: Scrambles message data based on key. Mathematically,

$$E : \mathscr{M} \times \mathscr{K} \rightarrow \mathscr{C}$$

$$E(m, k_e) = c$$

- Decryption: recovers message data,only when provided correct key. Mathematically,

$$D : \mathscr{C} \times \mathscr{K} \rightarrow \mathscr{M}$$

$$D(c, k_d) = m$$

- Desirable properties:
  - Easy to encrypt.
  - Difficult to invert without key.

Some Standard Ciphers

- Simple way, $c = m \oplus k$, $m' = c \oplus k = m \oplus k \oplus k = m$.

Some Standard Ciphers

- Simple way, $c = m \oplus k$, $m' = c \oplus k = m \oplus k \oplus k = m$.
- Symmetric key cryptosystems, i.e. $k_e = k_d$

Some Standard Ciphers

- Simple way, $c = m \oplus k$, $m' = c \oplus k = m \oplus k \oplus k = m$.
- Symmetric key cryptosystems, i.e. $k_e = k_d$
  - Block ciphers: AES,DES,IDEA

Some Standard Ciphers

- Simple way, $c = m \oplus k$, $m' = c \oplus k = m \oplus k \oplus k = m$.
- Symmetric key cryptosystems, i.e. $k_e = k_d$
  - Block ciphers: AES,DES,IDEA
  - Stream ciphers: RC4,FISH,SEAL

Some Standard Ciphers

- Simple way, $c = m \oplus k$, $m' = c \oplus k = m \oplus k \oplus k = m$.
- Symmetric key cryptosystems, i.e. $k_e = k_d$
  - Block ciphers: AES,DES,IDEA
  - Stream ciphers: RC4,FISH,SEAL
- Public key cryptosystems, i.e. $k_e \neq k_d$
  RSA,Rabbin,ECC. (Elliptic Curve Cryptosystem)

Some Standard Ciphers

- Simple way, $c = m \oplus k$, $m' = c \oplus k = m \oplus k \oplus k = m$.
- Symmetric key cryptosystems, i.e. $k_e = k_d$
  - Block ciphers: AES,DES,IDEA
  - Stream ciphers: RC4,FISH,SEAL
- Public key cryptosystems, i.e. $k_e \neq k_d$
  RSA,Rabbin,ECC. (Elliptic Curve Cryptosystem)
- Need of Mathematical Tools, i.e functions which are easy to compute and difficult to invert.

Preliminaries

- We say, $a \equiv b \mod (n)$, when n divides $(a - b)$.
- It is basically a remainder function.
- $84 \equiv 75 \mod (9)$, but in general, we will say $84 \equiv 3 \mod (9)$
- When $n = p$, some prime, p,Let, $\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}$.
- $(\mathbb{Z}_p^\times, \times_p)$: Multiplicative group.
- $g \in \mathbb{Z}_p^\times$ such that, $\{g, g^2, \ldots, g^{p-1}\} = \mathbb{Z}_p^\times$, then we say g is generator.

Hard Problems

- Integer Factorization Problem: (IFP)
  Given an integer $n = p * q$, product of two prime numbers, find prime factors, p, q.

Hard Problems

- Integer Factorization Problem: (IFP)
  Given an integer $n = p * q$, product of two prime numbers, find prime factors, p, q.
- Discrete Logarithm Problem (DLP)
  Let p be the prime number and g be the generator of $(\mathbb{Z}_p)^\times$.
  If, $a = g^x \mod (p)$, x is called as discrete logarithm of a.
  DLP is, given 'a' find discrete logarithm of 'a' in $(\mathbb{Z}_p)^\times$
  i.e. find x s.t. $g^x \mod (p) = a$.

Hard Problems

- **Integer Factorization Problem: (IFP)**
  Given an integer $n = p * q$, product of two prime numbers, find prime factors, p, q.
- **Discrete Logarithm Problem (DLP)**
  Let p be the prime number and g be the generator of $(\mathbb{Z}_p)^\times$.
  If, $a = g^x \mod (p)$, x is called as discrete logarithm of a.
  DLP is, given 'a' find discrete logarithm of 'a' in $(\mathbb{Z}_p)^\times$
  i.e. find x s.t. $g^x \mod (p) = a$.
- **Diffie-Hellman Problem: (DHP)**
  Let p be the prime number and g be the generator of $(\mathbb{Z}_p)^\times$.
  Given $g^a \mod (p)$,$g^b \mod (p)$, find $g^{ab} \mod (p)$

RSA

RSA Cryptosystem consists Three Primitives:

- Key Generation
- Encryption
- Decryption

Key Generation

1. Choose, p and q, two large primes.
2. Calculate: $n = p * q$. $\phi(n) = (p-1) * (q-1)$.
3. Choose e such that $g.c.d$ of e and $\phi(n)$ is 1.
4. Calculate d such that $ed \equiv 1 \mod (\phi(n))$.

RSA: Key Generation

- If *g.c.d* of a and b is 1, there exists unique x and y such that

$$ax + by = 1.$$

- Let, $a = e, b = \phi(n)$. Then, x will be required d.
  And this can be calculated using Extended Euclidian Algorithm.
- (e, n) is called public key or encryption key.
- (d, n) is called private key or decryption key.

RSA Contd...

Let, (e, n) be public key of A and (d, n) corresponding private key.
Message m, is such that $1 \leq m \leq n$

Encryption

When B want to send a m to A,
he will send
$c \equiv m^e \mod (n)$

Decryption

After receiving c,
A will retrieve message back using
$m' \equiv c^d mod(n)$

$$\begin{aligned} m' &\equiv c^d \\ &\equiv (m^e)^d \mod (n) \\ &\equiv m^{(ed)} \mod (n) \end{aligned}$$

When, $n = p * q$, from Number Theory, we have
$a^x = a^{(x+\phi(n)-1)} \mod (n)$
$m' \equiv m \mod (n)$.

Cracking RSA

- Look at Key generation. If somebody solves IFP, he can easily deduce decryption key.
- Note: But, given public key, if someboy can deduce private key doesn't implay he can factor n. i.e.
  Solving IFP $\Rightarrow$ Cracking RSA
  Reverse may not be true.
- Rabin Cryptosystem: As hard as IFP.

Factoring number

- Naive algorithm: Try all numbers 1 to $\sqrt{n}$.
- Time complexity: $O(\sqrt{n})$
- Suppose, $x^2 \equiv y^2 \mod n$ and $x \not\equiv \pm y \mod (n)$
  $\Rightarrow$ n divides $(x^2 - y^2)$ i.e. either $(x + y)$ or $(x - y)$.
- Who will give such x and y?

Factoring number

Dixton,quadratic sieving,number field sieving

- Choose $\mathscr{B}$, set of known prime numbers.
- Choose randomly, $x_1, x_2, \ldots, x_k$, s.t. $p(x_i) \equiv x_i^2 \mod (n)$ factors completely using primes in $\mathscr{B}$.
- Find $\{y_1 \ldots, y_l\} \subseteq \{x_1, x_2, \ldots, x_k\}$, such that

$$\prod_{i=1}^{l} y_i^2 \equiv \prod_{i=1}^{l} p(y_i) \mod (n)$$

  and, RHS of the above equation is square.
- Quadratic Sieving. Time Complexity: $O\left(exp(2\sqrt{2}\sqrt{\log n \log\log n})\right)$.
- Number Field Sieving. Time Complexity: $O\left(exp(c * (\log n)^{1/3}(\log\log n)^{2/3})\right)$.

Elliptic curve cryptosystems

- $y^2 = x^3 + ax + b$.
- Consider, set of all integer pair (x,y) s.t.

$$y^2 = x^3 + ax + b \mod (p),$$

  where p is prime.
- Group.
- We can use DLP.
- Till date, Time complexity: $O\left(exp(c(\log n)^{1/2}(\log\log n)^{1/2})\right)$.
- 1024 bit RSA security $\equiv$ 168 bit ECC security.

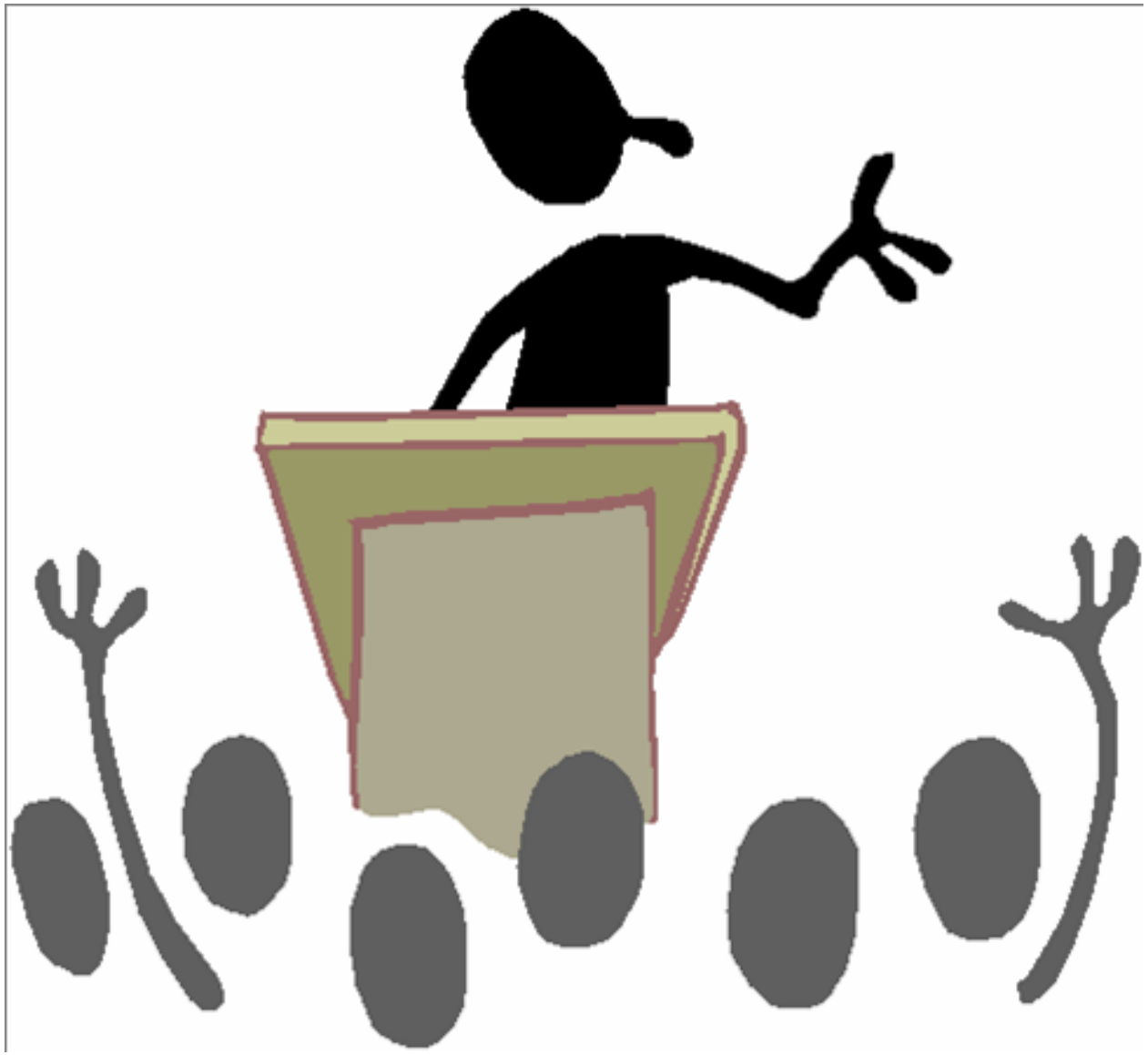
Conclusions

- Need of Mathematical functions in cryptography.
- Hard Problems.
- RSA Cryptosystem
- Integer Factoring.
- Elliptic Curve Cryptosystems.

References

- "Applied Cryptography", (2nd Ed.) by Bruce Schneier.
- "Handbook of Applied Cryptography", by Alfred Menezes, Paul van Oorschot and Scott Vanstone.
- "The Code Book", by Simon Singh.

Questions?



Thank You!!!