An Inquiry Into Modern Cryptography

Kannan Srinathan
IIIT-Hyderabad
What is cryptography about?
Why is cryptography important?
How to solve it (cryptography)?
CRYPTOGRAPHY

Is about `solving’ impossible problems
Cryptography …

… has to brazenly circumvent logical no-go theorems!
Sample No-Goes

Illustrating Logical No-Go (Russell’s Paradox): Let S be the set of all sets that do not contain itself. Does S belong to S?
Ans: Yes and No!

1. Should the machine know your password?
   Ans: Yes (for checking) and No (for secrecy)

2. Can you spend your digital cash?
   Ans: Yes (the original) and No (the copies)

3. Should there be CCTV cameras?
   Ans: Yes (for policing) and No (for privacy)
Cryptography is *Fascinating*

- Because ...

  ... no other field of science has so *pleasingly succeeded* in circumventing logical no-go results  ...
Sample “Successes” against Logical Impossibilities

1. Authenticity with Anonymity!

2. Blinding but Binding!

3. Compression without Collision!

4. Privacy Preserving Personalization!
Cryptography

Is therefore fundamental
Cryptography is *Fundamental*

- Because ...

... it has extended its success story by circumventing logical no-go theorems in other areas too ...
(S)ample Technical Benefits of Cryptography

- Coding Theory
  - Detecting 100% Adversarial Noise
- Distributed Computing
  - Fault-Tolerant Agreement
- Mathematics
  - What is a Proof?: Zero-Knowledge Proof Systems
- Algorithms
  - Pseudorandomness and Derandomization
Rest of the talk …

How To Solve It?

… the power of adversarial interference
The Cryptographic Method

- Understand the (original) impossibility

- Bring in another impossibility
  - In just about the correct proportion

- Make the impossibilities destructively interfere each other
  - … to make a solution possible!
Adversarial Interference
(has happened before crypto too)

- Randomized Algorithms
- Game Theory and Byzantium
Some Famous Adversities
(that enable cryptography)

- **Computational Adversity**
  - Eg. Limited resources

- **Physical Adversity**
  - Eg. Quantum and Relativistic Mechanics

- **Practical Adversity**
  - Eg. Scheduling and Software Bugs

- **Philosophical Adversity**
  - Eg. Clash of Fundamental Definitions
We’ll See One Example For Each Kind of Adversarial Interference

Four examples in all
Our First Example

Is Secure Communication a Cryptographic Problem?

Yes! It is a Logical No-Go!

Why?
Secure Communication is Impossible!

At time $t_0$
- $\text{Information@Receiver} = \text{Information@Adversary}$
  
Recall: Kerckhoff’s Principle

At every subsequent instant of time
- $\text{Information gained by receiver} = \text{Information gained by adversary}$
How to Circumvent the Impossibility?

Only Two Ways

At time $t_0$

Information@$\text{Receiver}$

is (perceived as) greater than

Information@$\text{Adversary}$

OR

At some subsequent instant of time

Information gained by receiver

is (perceived as) greater than

Information gained by adversary
The First Way …

Representation matters, indeed!
Natural Numbers, Efficiency of Operations and Modern Cryptography
Ease of Computation Depends on the Representation

It also depends on the operation!
Ease/Speed of Operation Depends on The Representation

- \( \text{viii} \times \text{xvi} = \text{cxxviii} \)
- \( 8 \times 16 = 128 \)
- \( 2^3 \times 2^4 = 2^7 \)

- \( \text{viii} + \text{xvi} = \text{xxiv} \)
- \( 8 + 16 = 24 \)
- \( 2^3 + 2^4 = 2^3.3 \)

- \( \text{viii} < \text{ix} \) is true
- \( 8 < 9 \) is true
- \( 2^3 < 3^2 \) is true
Top Three Most Frequent Operations

- Addition (+)
- Comparison (<)
- Multiplication (*)
## Why is the Decimal System Popular?

<table>
<thead>
<tr>
<th></th>
<th>Addition</th>
<th>Multiplication</th>
<th>Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROMAN</td>
<td>SLOW</td>
<td>SLOW</td>
<td>SLOW</td>
</tr>
<tr>
<td>DECIMAL</td>
<td>FAST</td>
<td>MEDIUM</td>
<td>FAST</td>
</tr>
<tr>
<td>PRIME PRODUCT</td>
<td>SLOW</td>
<td>FAST</td>
<td>SLOW</td>
</tr>
<tr>
<td>RESIDUE SYSTEM</td>
<td>FAST</td>
<td>FAST</td>
<td>MEDIUM</td>
</tr>
</tbody>
</table>
Is There a Representation Where all Common Operations are FAST?

Not Easy!
Slowness is ADVANTAGEOUS too!

Public Key Cryptography
Secure Communication

Choose Key K (in representation $R_1$)

$E_K(m)$

Key K

(in representation $R_2$)

$E^{-1}_K(E_K(m)) = m$

**In Representation $R_2$**

- Operation $E_K$ is FAST
- Operation $E_K^{-1}$ is VERY SLOW

**In Representation $R_1$**

- Operation $E_K^{-1}$ is FAST

**EXAMPLE RSA Cryptosystem**

$R_1$: Product of Primes

$R_2$: Decimal

$E_K$: Modular Exponentiation $m^e \mod K$
RECALL: How to Circumvent the Impossibility?

At time $t_0$

Information@Receiver

is (perceived as) greater than

Information@Adversary

OR

At some subsequent instant of time

Information gained by receiver

is (perceived as) greater than

Information gained by adversary
Our second example

Secure Communication in Quantum Channels

Natural Adversary
Quantum World: It’s *Bizarre!*
An Experiment with Photons

The Three Polarizers
The Photon Experiment
The Photon Experiment (Contd.)
Qubits

An Explanation
Qubits

- A quantum bit, or qubit, is a unit vector in a two dimensional complex vector space for which a particular basis has been fixed and is denoted by:

\[ \{ |0\rangle, |1\rangle \} \]

- Qubits can be in a superposition of $|0\rangle$ and $|1\rangle$ such as

\[ a|0\rangle + b|1\rangle \]

where $a$ and $b$ are complex numbers such that $|a|^2 + |b|^2 = 1$. 
Measuring a Qubit in the Basis

For the qubit

\[ a|0\rangle + b|1\rangle \]

the probability that the measured value is \( |0\rangle \) is

\[ |a|^2 \]

after which the state collapses to \( |0\rangle \) and

the probability that the measured value is \( |1\rangle \) is

\[ |b|^2 \]

after which the state collapses to \( |1\rangle \)
Qubit Model Correctly Predicts the Outcome of Photon Experiment and several other experiments too!
Quantum Secret Key Establishment Protocol

The Standard Setting
Quantum Secret Key Establishment Protocol

- Two bases are used, say $b_1$ and $b_2$.
- $S$ chooses a random base, and based on the bit to send, it sends a qubit prepared in the corresponding state.
- $R$ measures the qubit received, with a random base. If the base is different from what $S$ used, the bit is lost, else $R$ measures the actual bit (always so, only if an eavesdropper is absent!).

<table>
<thead>
<tr>
<th>Bit</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b_1$</td>
<td>↑</td>
<td>→</td>
</tr>
<tr>
<td>$b_2$</td>
<td>→</td>
<td>←</td>
</tr>
</tbody>
</table>
Our third example

Secure Communication in Noisy Channels

Practical Adversary
Secure AND

- Securely Computing $x \land y$ in GF(2)

Input: $x$
Input: $y$

Noise: Any 1 bit out of every block of 4 bits sent will be toggled

Fact: Perfectly Secure AND is impossible in a noiseless channel
Protocol for Secure AND

- A chooses four random bits, \( r_0, r_1, r_2, r_3 \) and sends them to B, who receives \( s_0, s_1, s_2, s_3 \)
  - One of the \( r_i \) is different from \( s_i \)
  - Three of the others are equal

- A and B compute the following 3-tuples respectively

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

- A (respectively B) multiplies the \( i^{th} \) row of matrix \( M \) with \( r_i \) (respectively \( s_i \)) to obtain a matrix \( M^A \) (resp. \( M^B \))

- A (resp. B) adds up the resultant 4 by 3 matrix \( M^A \) (resp. \( M^B \)) column-wise to obtain a 3-tuple \( T^A = (a_0, b_0, c_0) \) (resp. \( T^B = (a_1, b_1, c_1) \))
Our Last Example

Philosophical adversity
Some Important Philosophical Questions

- Who is *honest*?
- How can a software be at *fault*?
- What is a *proof*?
- What is *efficiency*?
- What is *intelligence*?
- What is *security*?
Can a cluster of insecure systems simulate security?

Welcome to blockchain!
Concluding Remarks

Adversarial interference is the key!
Thank You

Questions?