Exploration of Cryptography

Whitfield Diffie

Distinguished Visiting Professor

Zhejiang University

30 November 2020

Class 02
Basic Notions
of Cryptography

Cryptography

Protection of data by transformations that turn useful and comprehensible plaintext into scrambled and meaningless ciphertext under control of secret keys.

What Drives Cryptography?

Like every other field of engineering, cryptography responds to the requirements by using the available tools, driven by the imaginations of its practitioners.

Cryptography Guarantees Confidentiality

- Only authorized receivers who know secret keys can decrypt
- Eavesdropper may intercept message, but cannot understand it.

Cryptography Guarantees Authenticity

- Message sent by Intruder will decrypt to nonsense.
- Intruder may inject messages, but cannot ‘get them accepted.’

Cryptographic System

$$\boxed{\begin{array}{c}\text{Plain}\\\text{Text}\\\text{Space}\end{array}} \quad \underset{\{\mathcal{S}_k\}_{\{k\}\in\mathcal{K}}}{\longrightarrow} \quad \boxed{\begin{array}{c}\text{Cipher}\\\text{Text}\\\text{Space}\end{array}}$$

Representation of a Cipher

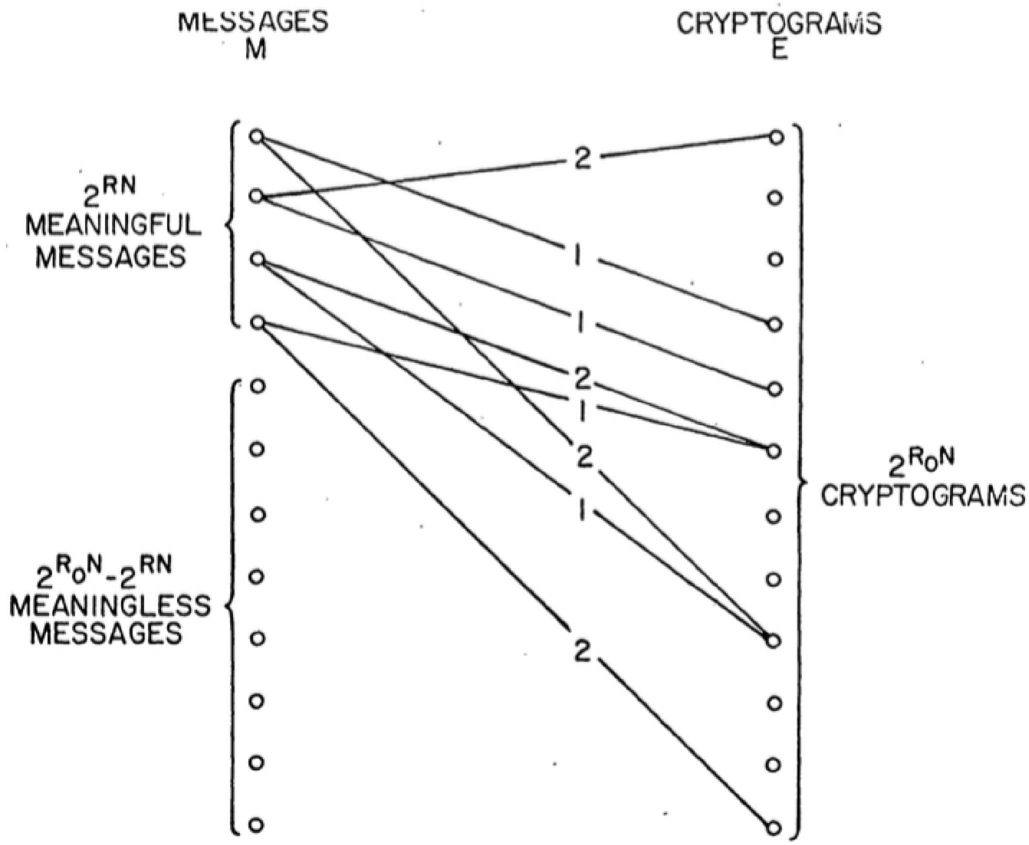

FIG. 1 REPRESENTATION OF A CIPHER

Representation of Encryption

Unkeyed map from plaintexts to plaintext representations.

Keyed map from plaintext representations to ciphertext representations.

Unkeyed map ciphertext representations to ciphertext.

Plaintext

Information In Usable

and Comprehensible Form

(Definition by intention.)

Examples of Plaintext

- Written human language
- Spoken Language
- Accounting Legers
- Seismic Data

Examples of Plaintext (Cont'd)

- Computer program
- Formal commands (EFT, C^2)
- Somebody else's ciphertext

Representations of Plaintext

- Messages drawn from a fixed set
- Fixed length strings over an alphabet
- Finite length strings ...

Characteristics of Plaintext

- Message (e.g., letter) frequencies
- Pair and triple frequencies
- Contact characteristics
- Gramatical restrictions

Ciphertext

Information in Useless

Scrambled Form

(Definition by intention.)

Characteristics of Ciphertext

Unpredictable (random) at some level.

Scrambled and Useless

- Unreadable
- ‘Destroyed’ by Alteration
- Looks Like Random Noise

Substitution

Permutation of the space of plaintexts.

Full Subsitution

Plaintext space, or message space, or alphabet: M of n elements.

$$k : M \mapsto M \qquad \text{invertible}$$

$$\text{Number of keys} = (\mathsf{Card}(M))!$$

where each $k \in S_{\mathsf{Card}(M)}$.

Examples of Full Substitution

- Monoalphabetic substitution on Roman (or ASCII, etc.) alphabet: S-box.

$$k : \{A, \ldots, Z\} \mapsto \{A, \ldots, Z\}$$

(Induces function on Roman-alphabet text.) each $k \in S_{26}$.

Examples of Full Substitution (cont'd)

- Prearranged message code

sell short	TXDNL
go public	PULID
fire CEO	HADOS
file Chap. 11	AMBIT
...	...

Examples of Full Substitution (cont'd)

- Substitution on letters
- Substitution on words
- Substitution on phrases
- Substitution on Sentences

Maximal and Minimal Substitutions

Minimal Substitution: The Cyclic Shifts

Let: $a \rightarrow 0, b \rightarrow 1, \ldots$ and let

$k \in \{0, \ldots, 25\}$ map $\ell \mapsto \ell + k$.

Full or Maximal Substitution

For any set $\{p\ 1, \ldots, p\ n\}$ of plaintexts

and any set of ciphertexts

$\{c\ 1, \ldots, c\ n\}$ there is a key such that

$k(p\ i) = c\ i$.

Transposition

Permute Elements of Message

`w h a t i s i n i t f o r m e`

`h m i i t s i o t w r n e a f`

Identification Friend or Foe

Mark XII IFF

Challenger	Responder
32-bit Random	32 bits in
Encrypt Locally	4 bits out

compare

General Systems and Specific Keys

- Cryptographic Systems
  - Standardized and Public

- Cryptographic Keys
  - Unique and Secret

Like Physical Locks and Keys

Cryptographic Systems

- Standardized
- Economy of Scale
- In Principle Public

Cryptographic Keys

- Very Large Supply
- Each Key Unique
- Must Be Kept Secret

All Secrecy Resides In Key

Primary and Secondary Keys

The primary key is the one changed most frequently, perhaps with every message.

The secondary key is changed less frequently, perhaps every day, week, or month.

Cryptanalysis

Produce Plaintext from Ciphertext (Analytic)

or

Produce Ciphertext from Plaintext (Synthetic)

(Without Prior Knowledge of the Key)

Analytic Cryptanalysis

Analytic Cryptanalysis

- Extract Information from Cryptograms

- Violates Confidentiality

- Better Known Problem

Synthetic Cryptanalysis

Synthetic Cryptanalysis

- Create False Messages

- Violates Authenticity

- Harder Problem

Analytic vs. Synthetic Cryptanalysis

Synthetic crypta can be much harder than analytic.

Rolling Code Speech Scrambler

- Filter Speech into multiple bands.
- Rearange the Bands.
- Change Rearangement several times a second.

Food for Thought

Can synthetic ever be easier than analytic?

Applications of Cryptanalysis

- Entertainment
- Production of Intelligence
- Certification of Systems

Cryptanalytic Circumstances

Cryptanalyst is Always Presumed to Know the General System

- Matter of Definition

- Sound Security Practice

Types of Attack

- Ciphertext Only
- Known Plaintext
- Chosen Plaintext

Ciphertext Only

- Statistics of Language
- Probable Words

Known Plaintext

- Common Words and Phrases

- Previously Secret Material

- Good Certification Assumption

Chosen Plaintext

- Best certification assumption
- Either plain or ciphertext
- Can be interactive

Oneway Functions

- Easy to Compute Forward

- Hard to Go Back

Easy to Raise Numbers to Powers

$$x \to x^7$$

Hard to Extract Roots

$$x \to \sqrt[7]{x}$$

Easy to Multiply

$$127 \times 997 = 126,619$$

Hard to Factor

$$126,619$$

Public Key Cryptography

- Keys Come In Inverse Pairs
- Given One — Can't Find the Other

Fundamental Property

- Public Key
  - In telephone directory
- Secret Key
  - In subscriber's safe (or cryptoequipment)

Solves Both Problems

Key Distribution: Encrypt With Public Key

Digital Signature: Encrypt With Secret Key

Signed and Sealed Message

$$\overbrace{\left\{\underbrace{\{message\}^{\substack{\text{Sender}\\ \text{Private Key}}},}_{\text{Signed}} SenderID\right\}^{\substack{\text{Receiver}\\ \text{Public Key}}}}^{\text{Sealed}}$$

Information Theory

- Information resolves uncertainty

- Perfect secrecy

- Ideal secrecy

Finite Automaton

A finite automaton consists of a set of states S, a set of inputs I, a set of outputs O, and a distinguished starting state S_0, together with two rules: a change of state map:

$$CS : I \times S \mapsto S$$

and an output map:

Finite Automaton (Cont'd)

$$Out : S \mapsto O \qquad \text{Moore}$$

or

$$Out : S \times O \mapsto O \qquad \text{Mealy}$$