Introduction to Cryptology

Lecture-06
Fundamentals of Secrecy Theory

04.04.2023, v45

Secrecy Theory

And Fundamentals of ciphering

Outlines

- Historical Overview
- Basic Definitions
- Shannon's Secrecy Theorem
- Perfect Secrecy „Vernam Cipher“
- Unicity Distance
- Secret Key Cipher Principle

Two interesting statements around security!

„The only system which is truly secure is one which is switched off , unplugged, locked in a titanium lined safe, buried in a concrete bunker, surrounded by nerve gas and very highly paid armed guards.
Even then, I wouldn't stake my life on it ....“

Gene Spafford - Computer Operations, Audit and Security Technology (COAST), Purdue University

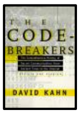
„If I am asked to stake my life on a cryptographic function,
I would not trust any function related to known mathematics“

Ulli Maurer – ETH Zürich, Swisserland

Scientific History of Cryptography

The origin of the word Cryptography (Greek: hidden word):
Is Cryptography an Art or or a Science ?

The scientific story of cryptography has **three** epochs:


(1967) Intensive historical treatment on secret communication

I. Conventional Cryptography as Art till 1949

- Julius Caesar Cipher
- Kaisiski “ The *Art* of Deciphering” 1863, ... Gauss
- Vernam (AT&T) 1926, *first* perfect/unbreakable system
- II world war 1945, Enigma, Hagelin .... Alan Turing

Less widely known in convectional public literature:
Jakob Alkindi Bagdad (801–873): "father of Islamic/Arabic philosophy“, Mathematician physician and musician. Presented first mathematical tools for cryptanalysis:

“Treaties on Extracting Cryptograms”, (Doc 4832 Sulaimania Library Istambul Turky)

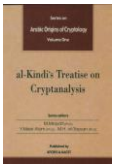
رسائل في استخراج المعمى: يقوب بن اسحق الكندي

David Khan: "Cryptology was born among the Arabs. They were the first to discover and write down the methods of cryptanalysis.”

Alkindi's Treaties on Cryptanalysis (استخراج المعمى) (873 AD)

- Classified different ciphering/deciphering techniques using a tree diagram

Figure 3.2 : A photocopy of the tree diagram of enciphering methods as appeared in al-Kindi's original
(Document No. 4832, as-Sulaymāniyya Library, Turkey)



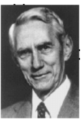
Translation Published by KACST in 2003

Scholars on history of science:
- Orientalist **Hellmut Ritter** (Istanbul Univ.)
- His student **PROF. FUAT SEZGIN** Uinv. Frankfurt
- **George Saliba** Columbia University
- … many others

PPT presentation: At Oxford University (2018)
“The Arabic Origins of Cryptology”
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiM4oqJ_pH-AhXySPEDHTDiBI0QFnoECAgQAQ&url=https%3A%2F%2Fmuslimheritage.com%2Fwp-content%2Fuploads%2F2018%2F05%2Fcryptology01.pdf&usg=AOvVaw0ymtbKqj6NzdH0KreCZqhS

- Legacy of other old cultures: Chines, Indian … crypto history !

Scientific Epochs and Breakthrough in Cryptography


1916-2001

2. Modern scientific epoch: (1949)
Shannon (AT&T) 1948 “A Mathematical Theory of Communication”

Shannon's Breakthrough in Communication Technology:
Error-free transmission is possible on noisy channels! $C = B \log_2 (1 + S/N)$

Shannon (AT&T) 1949 “Communication Theory of Secrecy System”
- proved mathematically that Vernam cipher is unbreakable
- Introduced the first modern scientific methodology in cryptography
- NO breakthrough in cryptography!

3. The breakthrough towards the modern Cryptology came in 1976
Diffie and Hellman introduced in 1976 the Public-Key Cryptography (Stanford University)

Diffie Hellman 's Breakthrough in Cryptography:
Secured transmission is possible on unsecured channels!

.... Any new Breakthrough expected ? !

BIG OPEN QUESTIONS

1. Is Security Measurable?
2. Is Security a Science, Art or Magic ?

Question raised by James L. Massey
Cryptography - Science or Magic?
MIT, October 1, 2001, Running Time: 00:57:10
https://techtv.mit.edu/videos/16442-cryptography-science-or-magic

Two Major Security Tasks

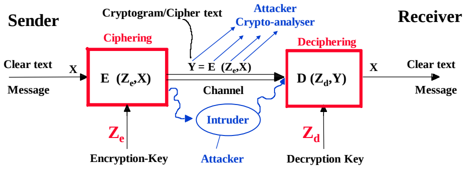
- ***Authentication***
  Securely identify an entity
- ***Secrecy***
  Keep data safe against illegal users

Security tasks require to deploy Cryptographic mechanisms to be realized
Cryptography is the science dealing with hiding information and data security questions

Conventional Secret Key Cryptography in Use

Fundamental Concepts

Cryptography : Basic definetions



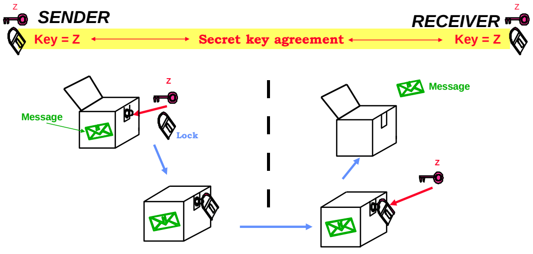
Cryptographic Attacks: Basic definetions

Type of attacks:
- Cipher text only attack
- Known plaintext attack
- Chosen plaintext attack
- Chosen ciphertext attack

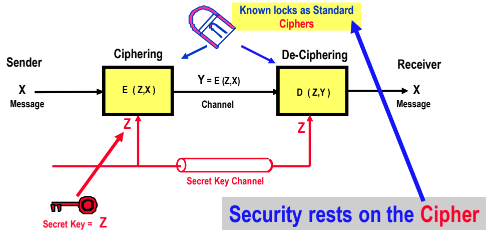
Chosen Cipher/Plain Text Attack: is mostly assumed as a basis to evaluate the quality of a cipher

A Fundamental Principle on Attacks:
Kerckhoff's Principle: A fundamental security evaluation assumption:
Attacker knows everything but not the key !

Secret Key Crypto-System : mechanical analog



Conventional Cryptography till 1976 : Secret Key systems



Security rests on the Cipher

Is Cryptographic Security Measurable ?

Yes and No !

Security measures adopted today:

System is unconditionally secure (perfect) :
System ***impossible*** to break with ***any*** means (whatever)
One not very practical system is known !

System is practically secure:
System ***possible*** to break but with very ***huge*** means
All modern practical systems fall under this category!

Non-sceientific statement

The Theory of "System Secrecy" is based on the Concept of

Information Entropy : a measure for information contents

Shannon 1949

"Probabilistic Model" of an information source:

Information Source $\xrightarrow{\text{Output}}$ $x \in \{Finite\, Set\, of\ Messages\ \ (SYMBOLS)\}$

Example: two symbole source (binary source):
Includes only two possible outputs for x,
that is: $x \in \{0,1\}$

P : Probability distribution function

$$if \quad P(x=0)=p \ then \quad P(x=1)=1-p$$

Example for M-symbol source:

$$x \in \{0,1,\ldots,M-1\} \qquad with \quad \sum P_i = 1$$

Measure of the Amount of Information (Entropy Unit)

Example for 1-bit information entropy

For instance, 0 denotes Head and 1 denotes Tail : or **vice versa**
The probability of Head is **0.5** and the probability of Tail is **0.5** too.

Fair coin flipping

The information entropy for that case is = **1 bit**
2 Possibilities which are equally probable!

Entropy is measured in **BITS**

Maximum entropy is attained by equal probabilities!

The Information Entropy Function : Shannon 1949

Amount of information in a message M having n possible combinations is defined by Shannon as **"Entropy" H(M)** where:

$$H(M) = \sum_{i=1}^{n} \ \mathrm{Prob}(M_i) \ \log_2 \frac{1}{\mathrm{Prob}(M_i)}$$ overall n-possible messages M_i

Maximum entropy of an information source having n possible symbols is attained **if all *n* combinations are equally probable**,
that is Prob(M_i) = 1/n for any i, Hence:

$$H(M) = \sum_{i=1}^{n} \ (1/n) \ \log_2 n$$
$$= n \bullet (1/n \ \ \log_2 n)$$
$$= \log_2 n$$

Again, *n* is the number of all possible combinations

Example 1:
M = 12 months of the year appear equally likely
H(*M*) = $\log_2 12 \approx 3.6$ bits

Example 2:
A k-bit key vector having 2^k equally probable key selections has an entropy of:
H(*M*) = $\log_2 2^k$ = k bits

The Theory of Perfect Secrecy Systems

Shannon 1949

If the entropy function for information source X: $H(X) = -\sum_{\{X\}} p_r(x_i) \, . \, \log_2 p_r(x_i)$

Where: $0 \le H(X) \le \log_2 t$ (for t possibilities for message X),
and If the key entropy is similarly H(Z) , then:

Shannon Condition for Perfect Security is $H(Z) \geq H(X)$

If the key is fully randomly selected (usuals practice), then key entropy (H(Z)
(a key having k-bits and all key-combinations are equally likely selected/used:

$$H(Z) = -2^k \ [\ (1/2^k) \ . \ \mathrm{Log}_2 (1/2^k) \ ]$$
$$H(Z) = k$$

In that case, the necessary condition for Perfect Security is : $k \geq H(X)$
or $k \geq$ Information length
as H(x) is at most as long as the information block length

Secrecy Theory and Alkindi's Contribution in Cryptanalysis

(استخراج المعمى)

(1000 years old mathematical treatment similar to Shannon's generalized modern entropy techniques)

Introduced for the first time how to use the probability distribution of letters to break ciphers

- Determining the statistical distribution of the frequency of letters in a particular natural language and made use of it to break a cipher by comparing the letter frequency in the cryptogram and natural text (showed an example of a text with 3667 letters)
  (for comparison: see Shannon's Entropy Concept and function in page 17-18)
- Indicated the importance that cryptogram must be sufficiently long to attain good accuracy (statistical significance).

Notice : Alkindi's treatise were dedicated to the central government in Bagdad (Calif Abu Al-abbas) The use of Cryptography was mainly to transfer confidential reports to the Caliph from the different widespread ruled territories (called "Bareed " service at that time)

Ref.: http://www.muslimheritage.com/

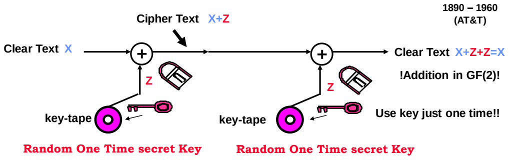
First and only known unbreakable Cipher

One-time-Pad OTP (Vernam Cipher)

Invented by Vernam (AT&T 1926)

Proved later to be impossible to break by Shannon (AT&T 1949)

Gilbert Vernam
1890 – 1960
(AT&T)

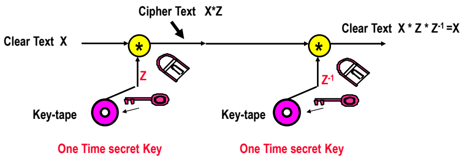


Unconditionally Secrure as : Key length = Clear text length (Shannon 1949)

$H(z) \geq H(X)$

Generalised One-Time Pad Cipher

System is also perfect for any Group < G, * >



Key length = Clear text length !!!
No key is repeatedly used!!

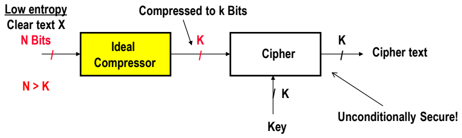
Improving Security by Message Compression

Enhance security by reducing redundancy

Perfect security always possible iff: Key length = Clear text length that is K=N

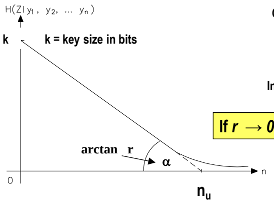
Natural languages have inherently low entropy as many information sources

if N > K then, try to make K=N by reducing N trough data compression to improve clear test entropy (reduce redundancy)



Unicity Distance: Minimum required ciphertext to break a cipher

Key equivocation function: $H(Z|y_1, y_2, y_3 \ldots y_n)$ for non-randomized cipher



k = key size in bits

Cipher Unicity Distance $n_u = \frac{H(Z)}{r} = \frac{K}{r}$

Information Redundancy $r = \frac{N - H(X)}{N}$

If $r \longrightarrow 0$, then $n_u \longrightarrow \infty$ => Cipher is perfect

n = number of the sent cryptogram symbols

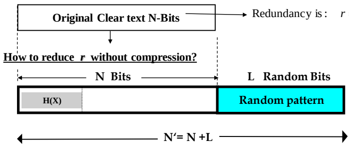
Unicity Distance n_u : is the minimum amount of ciphertext symbols which in principle can determin the secret key in a ciphertext only attack

Or: Expected minimum amount of ciphertext needed for brute-force to break a cipher

Plain Text *Padding technique to improve security*

(by increasing the unicity distance)

As larger uniucity distance means higher security, therefore a technique is proposed to increase the unicity distance by appending random unknown clear text as follows:


Original Clear text N-Bits
How to reduce r without compression?
N Bits
L Random Bits
H(X)
Random pattern
N'= N +L

Redundancy is : $r = \frac{N - H(X)}{N}$

$n_u = \frac{H(Z)}{r} = \frac{K}{r}$

New clear text N+L Bits

New Redundancy is : $r' = \frac{N' - H'(X)}{N'} = \frac{N + L - (H(x) + L)}{N + L} = r\frac{N}{N + L}$

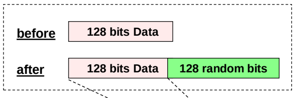
New unicity distance: $n'_u = \frac{K}{r'}$

$n'_u = \frac{N + L}{N} n_u$

Example: A block cipher having a key size of 128 bits is encrypting a clear text with a block length of 128 bits. The clear text redundancy is r=0.8.

1. Compute the cipher‘s unicity distance n_u and the clear text entropy.
2. The „unicity distance was doubled by appending L random bits to the clear text block. Compute L and the new clear text entropy.
3. After all the above cipher changes an observer was able to watch 1000 cipher text bits. Would the observer with unlimited resources theoretically be able to uniquely break the cipher in that case ? Give a reasoning for your answer.

Solution:



K= 128 Bits, H(x)=? Bits, r = 0.8

1. Unicity distance $\boxed{n_u = \frac{K}{r}}$ = 128/0.8 = 160 Bits (the cipher can be theoretically broken after 160 cipher bits)

   As r = [N – H(x)] / N
   => N . r = N – H(x) => entropy $\boxed{H(x) = N \cdot (1-r)}$ => H(x) = 128 · (1-0.8) = 25.6 Bits

   Usefull Iformation part of the 128 bits are only 25 bit !

2. $n'_u = [(N + L) / N] \cdot n_u$

   $2 \cdot 160 = [(128 + L) / 128] \cdot 160$

   => L = 128 Bits

   H‘(x) = L + H(x) = 128 + 25,6 = 153.6 bits

3. The observer can theoretically break the cipher as the number of the observed cryptogram bits (1000 bits) is more than the unicity distance (320 bits) of the cipher.