Perfect Cipher

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
gianluca.dini@unipi.it

1

Towards a secure cipher

- Attacker's ability: (one) cipher-text only attack
- Security requirements
  - Attacker cannot recover the secret key
  - Attacker cannot recover the plaintext
- Intuition of perfectly secure cipher
  - Regardless of *any prior information* the attacker has about the plaintext, the cyphertext should leak *no additional information* about the plaintext

2

Preliminaries

- Random variable, probability distribution
- Conditional probability
  - $\Pr[A|B] = \Pr[A \wedge B]/\Pr[B]$
- Law of total probability
  - $\{E_i\}$ are a *partition* of all possible events
    - For all i, j, $i \neq j$, E_i and E_j are pairwise impossible
    - At least some E_i occurs
  - For any event A, $\Pr[A] = \Sigma_i \Pr[A \wedge E_i] = \Sigma_i \Pr[A|E_i] \times \Pr[E_i]$
- Bayes' Theorem
  - $\Pr[A|B] = \Pr[B|A] \times \Pr[A]/\Pr[B]$

A probabilistic approach

- Message M is a random variable
  - Plaintext distribution
  - Example
    - Pr[M = "attack today"] = 0.7
    - Pr[M = "don't attack] = 03
  - Prior knowledge of the attacker
- Gen() defines a probability distribution over **K**
  - $\Pr[K = k] = \Pr[k \leftarrow \text{Gen}()]$
- Random variables M and K are independent

A probabilistic approach

- Ciphertext generation process
  - Choose a message m
  - Generate a key k, k ← Gen()
  - Compute c ← $E_k(m)$
- The ciphertext is a random variable C
- Encryption defines a distribution over the ciphertext **C**

Perfect secrecy (informal)

- We formalize «information about the plaintext» in terms of probability distribution
- The adversary's *a-priori* knowledge of the plaintext distribution, i.e. before observing a ciphertext, and the adversary's *a-posteriori* knowledge of the plaintex distribution, i.e. after observing the ciphertext, must be equal

Perfect secrecy (Shannon, 1949)

- Definition of Perfect secrecy – For every distribution over **M**, every p in **M**, every c in **C**, with Pr[C = c] > 0, it holds Pr[M = m | C = c] = Pr[M = m]

Shannon's Theorem

- Shannon's Theorem – In a perfect cipher, |**K** | ≥ |**M**|
  - i.e., the number of keys cannot be smaller than the number of messages
  - Proof. By contradiction.
    a) Let |**K**|<|**M**|
    b) It must be |**C**| ≥ |**M**| or, otherwise, the cipher is not invertible
    c) Therefore, |**C**| > |**K**|
    d) Select m in **M**, s.t., Pr[M = m] ≠ 0; $c_i \leftarrow E(k_i, m)$ for all k_i in **K**
    e) Because of c), there exists at least one c s.t. $c \neq c_i$, for all i
    f) Therefore Pr[M = m|C = c] = 0, that is different of Pr[M = m]

Unconditional security

- Perfect secrecy is equivalent to unconditional security
  - An adversary is assumed to have infinite computing resources
  - Observation of the CT provides the adversary no information whatsoever
- Necessary conditions
  - Key bits are truly randomly chosen
  - Key len $\geq$ msg len (Shannon theorem)

Perfect indstinguishability

- Definition – An encryption scheme Π = (G, E, D) over (**K**, **M**, **C**) has perfect indistinguishability iff
  - For all $m_1, m_2 \in$ **P**, $|m_1| = |m_2|$
  - with k ← Gen() (uniform)
  - For all $c \in$ **C**, $Pr[E(k, m_1) = c] = Pr[E(k, m_2) = c]$
- Fact – Π has perfectly indistinguishability iff it is perfectly secure

Perfect Cipher

ONE-TIME PAD

11

One Time Pad

UNIVERSITÀ DI PISA

- Patented in 1917 by Vernam
  - Known 35 years earlier
- Proven perfect by Shannon in 1949
- Moscow-Washington “red telephone”
  - In reality a secure direct communication link
    - Teletype, fax machine, secure computer link (email)
  - Never a telephone (not even red)

12

Preliminary

UNIVERSITÀ DI PISA

- Or-exclusive (xor)
  - Truth table

x	y	z = x ⊕ y
0	0	0
0	1	1
1	0	1
1	1	0

  - Matematically
    - $z = x \oplus y = (x + y) \bmod 2$

March 22 Perfect cipher 13

13

One Time Pad

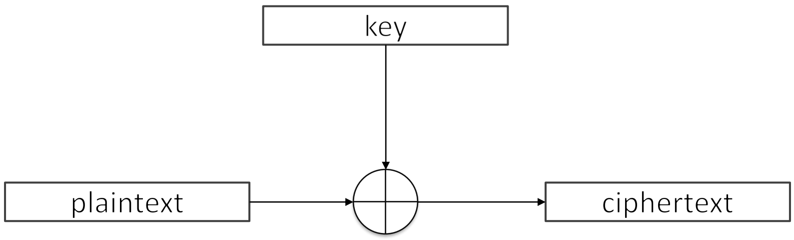
UNIVERSITÀ DI PISA

- Assumptions
  - Let x be a t-bit message, i.e., $x \in \{0,1\}^t$
  - Let k be a t-bit key stream, $k \in \{0, 1\}^t$, where each bit is truly random chosen
- Encryption
  - For all i in [1,…,t], $y_i = m_i \oplus k_i$ i.e., $y_i = m_i + k_i \bmod 2$
- Decryption
  - For all i in [1,…, t], $x_i = c_i \oplus k_i$, i.e., $x_i = y_i + k_i \bmod 2$
- Consistency property can be easily proven

March 22 Perfect cipher 14

14

One-Time Pad



Xor is a good encryption function

- Theorem – Let X be a random variable over $\{0, 1\}^n$, and K an independent uniform variable over $\{0,1\}^n$. Then, $Y = X \oplus K$ is uniform over $\{0,1\}^n$.
  - Proof (for n = 1).
    - Let $Pr[X = 0] = X0$, $Pr[X = 1] = X1$, $X0 + X1 = 1$
    - $Pr[Y = 0] =$
      $= Pr[(X = 0)\wedge(K = 0)] + Pr[(X = 1)\wedge(K = 1)] =$
      $= Pr[X = 0]\times Pr[K = 0] + Pr[X = 1] \times Pr[K = 1] =$
      $= X0 \times 0.5 + X1 \times 0.5 = 0.5 \times (X0 + X1) =$
      $= 0.5$

OTP has perfect secrecy

- Theorem – OTP has perfect secrecy
  - Proof
    a) $\Pr[M = m | C = c]$ = (Bayes law)
    $= \Pr[C = c \mid M = m] \times \Pr[M = m]/\Pr[C = c]$
    b) $\Pr[C = c]$ = (Total probability law)
    $= \Sigma_i \Pr[C = c | M = m_i] \times \Pr[M = m_i] =$
    $= \Sigma_i \Pr[K = c \oplus m_i] \times \Pr[M = m_i] =$
    $= \Sigma i\, 2^{-k} \times \Pr[M = m_i] = 2^{-k}$
    c) Put b) into a)
    $\Pr[M = m | C = c] =$
    $= \Pr[K = c \oplus m] \times \Pr[M = m]/2^{-k}$
    $= 2^{-k} \times \Pr[M = m]/2^{-k} =$
    $\Pr[M = m]$

17

OTP has perfect secrecy: intuition

- **c[i] = m[i] + k[i] mod 26**
- **m = "SUPPORT JAMES BOND"**

m =	S	U	P	P	O	R	T	J	A	M	E	S	B	O	N	D
k =	W	C	L	N	B	T	D	E	F	J	A	Z	G	U	I	R
c =	O	W	A	C	P	K	W	N	F	V	E	R	H	I	V	U

c =	O	W	A	C	P	K	W	N	F	V	E	R	H	I	V	U
k' =	M	W	L	J	V	T	S	E	F	J	A	Z	G	U	I	R
m =	C	A	P	T	U	R	E	J	A	M	E	S	B	O	N	D

19

Pros and Cons

UNIVERSITÀ DI PISA

- Pros
  - Unconditionally secure
    - A cryptosystem is unconditionally or information-theoretically secure if it cannot be broken even with infinite computational resources
  - Very fast enc/dec
  - Only one key maps m into c

March 22 Perfect cipher 20

20

Pros and Cons

UNIVERSITÀ DI PISA

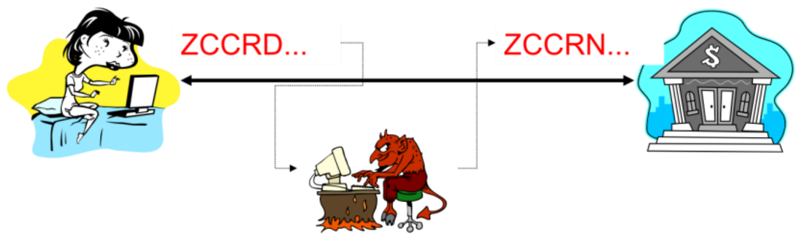
- Cons
  - Long keys: unpractical!
    - Key len == msg len
  - Keys must be used once: avoid two-time pad!
    - Let C1 = M1 xor K and C2 = M2 xor K => C1 xor C2 = M1 xor M2
  - A Known-PlainText attack breaks OTP
    - Given (m, c) => k = m xor c
  - OTP is malleable
    - Modifications to cipher-text are undetected and have predictable impact on plain-text

March 22 Perfect cipher 21

21

OTP is malleable

m =	D	A	R	E	C	E	N	T	O	E	U	R	O	A	B	O	B
k =	W	C	L	N	B	T	D	E	F	J	A	Z	G	U	I	R	X
c =	Z	C	C	R	D	X	Q	X	T	N	U	Q	U	U	J	F	Y



c' =	Z	C	C	R	N	B	O	P	J	N	U	Q	U	U	J	F	Y
k =	W	C	L	N	B	T	D	E	F	J	A	Z	G	U	I	R	X
m =	D	A	R	E	M	I	L	L	E	E	U	R	O	A	B	O	B

March 22 Perfect cipher 22

22

Malleability

- Malleability
  - A crypto scheme is said to be malleable if the attacker is capable of transforming the ciphertext into another ciphertext which leads to a known transformation of the plaintext
    - The attacker does not decrypt the ciphertext but (s)he is able to manipulate the plaintext in a predictable manner

March 22 Perfect cipher 23

23

On OTP malleability

- Attack against integrity
  - Alice sends Bob: $c = p \oplus k$
  - The adversary
    - intercepts c and
    - transmits Bob $c' = c \oplus r$, with r called *perturbation*
  - Bob
    - receives c'
    - Computes $p' = c' \oplus k = c \oplus r \oplus k = p \oplus k \oplus r \oplus k$ so obtaining $p' = p \oplus r$
    - The perturbation goes undetected and
    - The perturbation has a predictable impact on the plaintext

March 22 Perfect cipher 24

24

Example 1

- Shift cipher
  - K = {0, …, 26}, Pr[K = k] = 1/26
  - Pr[M = ‘a’] = 0.7; Pr[M = ‘z’] <0 0.3 (a-priori distribution)
  - Compute Pr[C = ‘b’]
    - Result = 1/26

March 22 Perfect cipher 25

25

Example 2

- Shift cipher
  - K = {0, …, 26}, Pr[K = k] = 1/26
  - m1 = «one», m2 = «ten»
  - Pr[M = m1] = Pr[M = m2] = 0.5 (a-priori distribution)
  - Compute Pr[C = «rqh»]
    - Result = 1/52

March 22 Perfect cipher 26

26

Example 3

- Shift cipher
  - K = {0, …, 26}, Pr[K = k] = 1/26
  - m1 = «one», m2 = «ten»
  - Pr[M = m1] = Pr[M = m2] = 0.5 (a-priori distribution)
  - Compute Pr[M=«ten»|C = «rqh»]
    - Result = 0 that is different of Pr[M = «ten»]

March 22 Perfect cipher 27

27

Example 4

- Shift cipher
- Message distribution
  - Pr[M = «hi»] = 0.3
  - Pr[M = «no»] = 0.2
  - Pr[M = «in»] = 0.5
- Compute Pr[M = «hi»|C = «xy»]
  - Pr[M=«hi»|C=«xy»] = (Bayes' law) =
    = Pr[C = «xy»|M=«hi»]·Pr[M=«hi»]/Pr[C=«xy»]
  - Pr[C = «xy»|M=«hi»] = Pr[K = 16] = 1/26 (continue)

Example 4 continued

- Compute Pr[M = «hi»|C = «xy»]
  - Pr[C = «xy»] =
    = Pr[C=«xy»|M=«hi»]·Pr[M=«hi»]+
    Pr[C=«xy»|M=«no»]·Pr[M=«no»]+
    Pr[C=«xy»|M=«in»]·Pr[M=«in»] =
    = (1/26)·0.3+ (1/26)·0.2+ 0·0.5 =
    = 1/52
  - Pr[M = «hi»|C = «xy»] = (1/26)·0.3/(1/52) = 0.6
    ≠ Pr[M = «hi»]
- Shift cipher is not perfect