STEVENS
INSTITUTE OF TECHNOLOGY
1870

CS396: Security, Privacy & Society

Fall 2022

Lecture 7: Cryptographic System I

Instructor: Abrar Alrumayh

September 19, 2022

The one-time pad

The one-time pad: A perfect cipher

A type of "<u>substitution</u>" cipher that is "**<u>absolutely unbreakable</u>**"

- invented in 1917 Gilbert Vernam and Joseph Mauborgne
- "substitution" cipher
  - **individually** replace plaintext characters with **shifted** ciphertext characters
  - **independently** shift each message character in a **random** manner
    - to encrypt a plaintext of length n, use n uniformly random keys $k_1, \ldots, k_n$
- "absolutely unbreakable"
  - **perfectly secure** (when used correctly)
  - based on message-symbol specific **independently random** shifts

The one-time pad (OTP) cipher

- Let **n** be an integer = of the plaintext messages.
- Message space **M** := $\{0, 1\}^n$ length (bit-strings of length n)
- Key space **K** := $\{0, 1\}^n$ (bit-strings of length n)
- **The key is as long as the message**

Fix n to be any positive integer; set $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$

- **Gen**: choose n bits uniformly at random (each bit independently w/ prob. .5)
  - Gen $\rightarrow \{0,1\}^n$
- **Enc**: given a key and a message of equal lengths, compute the bit-wise **XOR**
  - $Enc(k, m) = Enc_k(m) \rightarrow k \oplus m$ (i.e., mask the message with the key)
- **Dec**: compute the bit-wise XOR of the key and the ciphertext
  - $Dec(k, c) = Dec_k(c) := k \oplus c$
- Correctness Deck(Enck(m))
  - trivially, $k \oplus c = k \oplus k \oplus m = 0 \oplus m = m$

OTP is perfectly secure (using Definition 2)

For all n-bit long messages m_1 and m_2 and ciphertexts c, it holds that

$$\Pr[\, E_K(m_1) = c \,] \quad = \quad \Pr[\, E_K(m_2) = c \,],$$

where probabilities are measured over the possible keys chosen by Gen.

Proof

- events "$\mathrm{Enc}_K(m_1) = c$", "$m_1 \oplus K = c$" and "$K = m_1 \oplus c$" are equal-probable
- K is chosen at random, irrespectively of m_1 and m_2, with probability 2^{-n}
- thus, the ciphertext does not reveal anything about the plaintext

OTP characteristics

A "substitution" cipher

- encrypt an n-symbol m using n uniformly random "shift keys" $k_1, k_2, \ldots, k_n$

2 equivalent views

- $\mathcal{K} = \mathcal{M} = \mathcal{C}$
- "shift" method

view 1 $\{0,1\}^n$	or	view 2 G, (G,+) is a group
bit-wise XOR ($m \oplus k$)		addition/subtraction (m +/- k)

Perfect secrecy

- since each shift is random, every ciphertext is equally likely for any plaintext

Limitations (on efficiency)

- "shift keys" (1) are **as long as messages** & (2) **can be used only once**

Perfect, but impractical

In spite of its perfect security, OTP has two notable weaknesses

- the key has to be **as long as** the plaintext
  - limited applicability
  - key-management problem
- the key **cannot be reused** (thus, the “one-time” pad)
  - if reused, perfect security is not satisfied
    - e.g., reusing a key once, leaks the XOR of two plaintext messages
    - this type of leakage can be devastating against secrecy

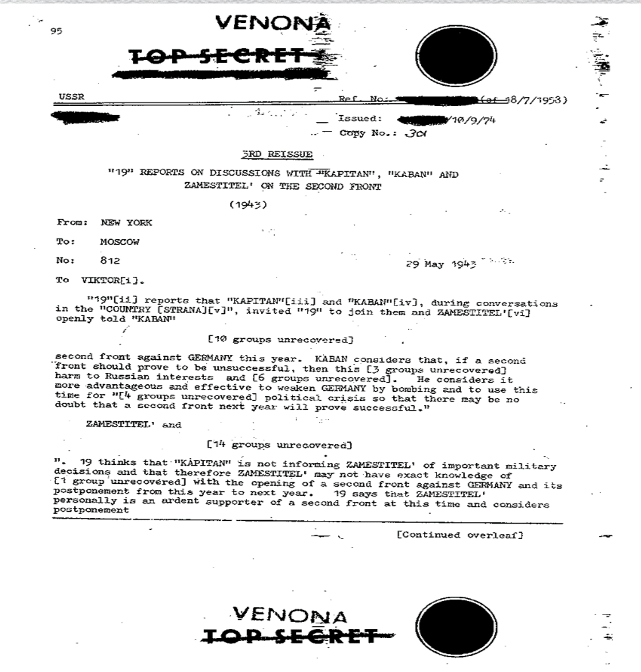
These weakness are detrimental to secure communication

- securely distributing fresh long keys is as hard as securely exchanging messages…

Importance of OTP weaknesses

Inherent trade-off between efficiency / practicality Vs. perfect secrecy

- historically, OTP has been used efficiently & insecurely
  - repeated use of one-time pads compromised communications during the cold war
    - NSA decrypted Soviet messages that were transmitted in the 1940s
    - that was possible because the Soviets reused the keys in the one-time pad scheme
- modern approaches resemble OTP encryption
  - efficiency via use of pseudorandom OTP keys
  - “almost perfect” secrecy



95

VENONA

~~TOP SECRET~~

[redacted]

[redacted]

USSR

Ref. No.: [redacted] (of 18/7/1953)

[redacted]

Issued: [redacted]/10/9/74

Copy No.: 301

3RD REISSUE

"19" REPORTS ON DISCUSSIONS WITH "KAPITAN", "KABAN" AND ZAMESTITEL' ON THE SECOND FRONT

(1943)

From: NEW YORK

To: MOSCOW

No: 812

29 May 1943

To VIKTOR[i].

"19"[ii] reports that "KAPITAN"[iii] and "KABAN"[iv], during conversations in the "COUNTRY [STRANA][v]", invited "19" to join them and ZAMESTITEL'[vi] openly told "KABAN"

[10 groups unrecovered]

second front against GERMANY this year. KABAN considers that, if a second front should prove to be unsuccessful, then this [3 groups unrecovered] harm to Russian interests and [6 groups unrecovered]. He considers it more advantageous and effective to weaken GERMANY by bombing and to use this time for "[4 groups unrecovered] political crisis so that there may be no doubt that a second front next year will prove successful."

ZAMESTITEL' and

[14 groups unrecovered]

". 19 thinks that "KAPITAN" is not informing ZAMESTITEL' of important military decisions and that therefore ZAMESTITEL' may not have exact knowledge of [1 group unrecovered] with the opening of a second front against GERMANY and its postponement from this year to next year. 19 says that ZAMESTITEL' personally is an ardent supporter of a second front at this time and considers postponement

[Continued overleaf]

VENONA

~~TOP SECRET~~

[redacted]