CISC 3325 - INFORMATION SECURITY

Quantum Cryptography

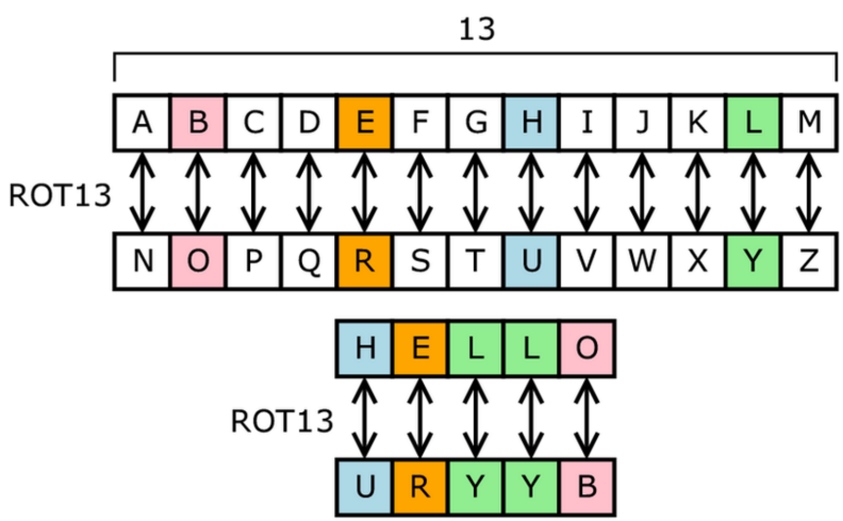
Quantum Cryptography

- In a way a variant of the idea behind a one-time pad
  - the only provably unbreakable encryption scheme
  - Requires two copies of a long string of unpredictable numbers, one copy each for the sender and receiver
  - The sender combines a number with a unit of plaintext to produce the ciphertext
    - If the numbers are truly unpredictable, the attacker cannot separate the numbers from the ciphertext

ONE-TIME PAD

Substitution Ciphers

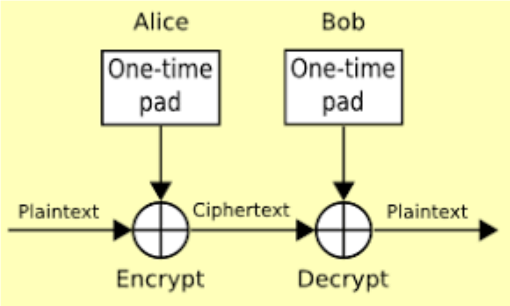
- Traditional ciphers, used for 1000s of years
  - Not used in modern systems anymore
- One popular substitution “cipher” for some Internet posts is ROT13.



Public domain image from http://en.wikipedia.org/wiki/File:ROT13.png

One-Time Pads

- One variation of substitution cipher is theoretically unbreakable.
  - The one-time pad was invented in 1917 by Joseph Mauborgne and Gilbert Vernam
  - We use a block of shift keys, $(k_1, k_2, \ldots, k_n)$, to encrypt a plaintext, M, of length n
    - with each shift key being chosen uniformly at random
- Since each shift is random, every ciphertext is equally likely for any plaintext.



https://programmingcode4life.blogspot.com/2015/10/one-time-pad-cipher.html

Conversion Table

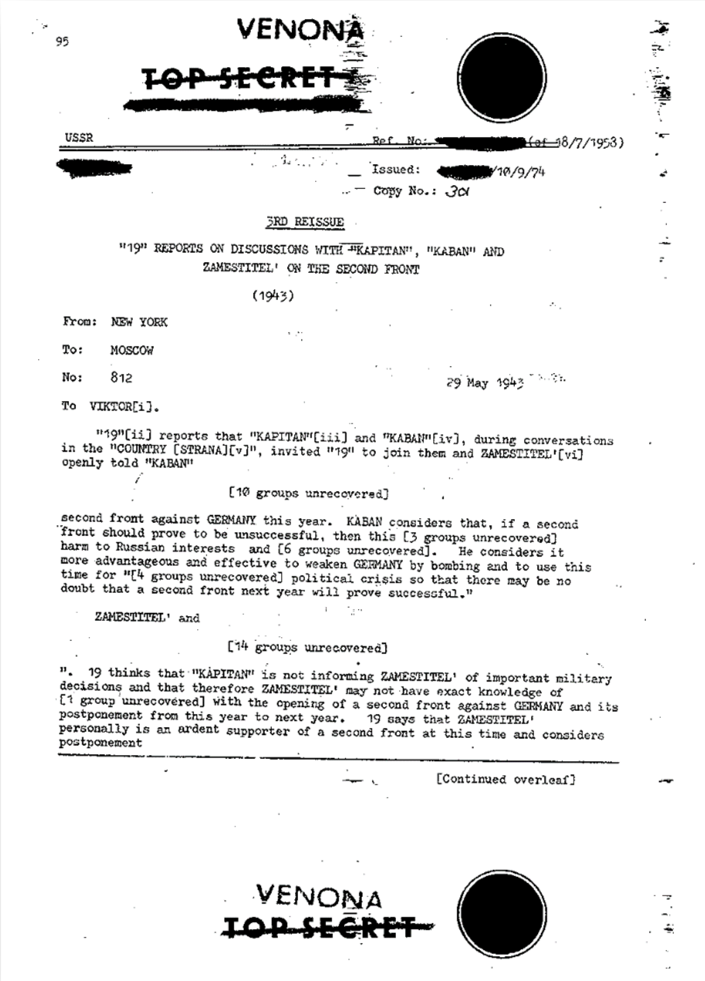
Conversion Table

A = 1	K = 11	U = 21
B = 2	L = 12	V = 22
C = 3	M = 13	W = 23
D = 4	N = 14	X = 24
E = 5	O = 15	Y = 25
F = 6	P = 16	Z = 26
G = 7	Q = 17	
H = 8	R = 18	
I = 9	S = 19	
J = 10	T = 20	

Weaknesses of the One-Time Pad

While perfect secure in theory, one-time pads have some weaknesses

- The key has to be as long as the plaintext
- Keys can never be reused
  - Repeated use of one-time pads allowed the U.S. to break some of the communications of Soviet spies during the Cold War.



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]

Quantum Cryptography

- In a way a variant of the idea behind a one-time pad
  - the only provably unbreakable encryption scheme
  - Requires two copies of a long string of unpredictable numbers, one copy each for the sender and receiver
  - The sender combines a number with a unit of plaintext to produce the ciphertext
    - If the numbers are truly unpredictable, the attacker cannot separate the numbers from the ciphertext

Quantum Cryptography

- Difficulty with this approach:
  - There are few sources of sharable strings of random numbers
  - Quantum cryptography addresses both problems, generating and communicating numbers
- How?
  - Transmit a series of photons
    - Produces an unpredictable string

Quantum Cryptography

FIGURE 12-9 Transmission of Photons

Implementation

- Technical difficulties still exist
- Scheme not put yet into practice
- Experimental implementations of quantum cryptography are still in the laboratories

QUANTUM COMPUTING AND SECURITY

Why quantum computing could make today's cybersecurity obsolete

https://www.weforum.org/agenda/2019/07/why-quantum-computing-could-make-todays-cybersecurity-obsolete/

Quantum Computing and Security

- What is considered safe encryption today will soon be undermined by quantum computing.
- Estimated it may take quantum power of 4,000 quantum bits (Qubits)
  - to break today's ”strong” encryption keys.

Quantum Computing and Security

- Quantum computers are not there yet.
- Estimates suggest we may see this capability by 2023
  - Will take longer for these machines to become reliable.
  - However, weaker encryption algorithms may be threatened sooner.

Rise of the Hackers

- Rise of the Hackers

- Questions?