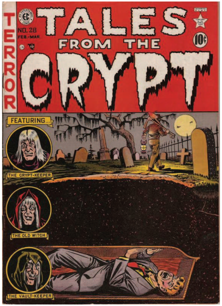
Cryptography, Cryptanalysis, Cryptology

Çetin Kaya Koç

http://cs.ucsb.edu/~koc
koc@cs.ucsb.edu

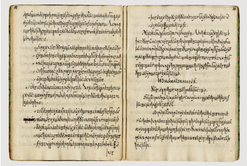
Terminology - Old & New

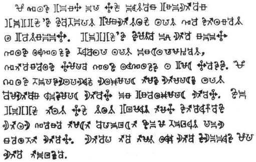
- Greek, Latin: kruptē, crypta (vault, burial chamber)
  crypt, to encrypt, to decrypt, encryption, decryption, encryption algorithm, decryption algorithm, cryptography, cryptanalysis, cryptology



Terminology - Old & New

- Arabic, Latin, French: șifr, , cifra, cifre (zero, empty)
  cipher, to encipher, to decipher, ciphertext, plaintext





- Informal: code, to encode, to decode, coding algorithm, secret codes

Codes - Error Detection & Correction

- In coding theory: The adversary is the Nature
- You want to send a piece of data over a channel
- The sender gives her data to the channel (encoding)
- The Nature attacks (indiscriminately) and may flip, destroy or duplicate bits
- The receiver obtains the "received" data
- The receiver wants the intended message (correct data)
- Error detection: Is the received data correct? Yes or No
- Error correction: Can you get the correct data from the received data?

Cryptography - Achieve Confidentiality

- In cryptology: The Adversary is another intelligent being
- The sender wants to send a piece of data over a channel
- The sender gives her data to the channel (encryption)
- The Adversary is always present
- The receiver obtains the received data (decryption)
- What did the Adversary learn?
- Is the data still confidential?

Cryptanalysis Scenarios - Kerckhoffs' Principle

Kerckhoffs' Principle:

The adversary knows the algorithm

Auguste Kerckhoffs (1835-1903) was a Dutch linguist and cryptographer who was a professor of languages at the École des Hautes Études Commerciales in Paris in the late 19th century.

Cryptanalysis Scenarios - Ciphertext & Plaintext

- Ciphertext only: $C_1, C_2, C_3, \ldots$
- Known plaintext: A set of (M_i, C_i) for $i = 1, 2, 3, \ldots, n$
- Chosen plaintext: Choose any M_i and obtain C_i for $i = 1, 2, 3, \ldots, n$
- Chosen ciphertext: Choose any C_i and obtain M_i for $i = 1, 2, 3, \ldots, n$
- Chosen text: Chosen plaintext + Chosen ciphertext
- Batch versus Adaptive chosen text
- "Lunchtime attacks"

Cryptographic Algorithms

For every cryptographic algorithm (cipher):

- Describe and understand the algorithm, input/output encoding scheme, encryption and decryption algorithms
- Block cipher vs stream cipher
- Input/output (plaintext/ciphertext) size
- Key size, key space, and key space size
- HW/SW platforms, performance issues → applied cryptography
- Cryptanalysis

Cryptanalysis Scenarios

- CO: Ciphertext Only; $C_1, C_2, C_3, \ldots$ [all ciphertexs]
- KP: Known Plaintext: A set of (M_i, C_i) for $i = 1, 2, \ldots, n$
- CP: Chosen Plaintext: Choose any M_i and obtain C_i for $i = 1, 2, \ldots, n$
- CC: Chosen Ciphertext: Choose any C_i and obtain M_i for $i = 1, 2, \ldots, n$
- CT: Chosen Text: Chosen plaintext + Chosen ciphertext

Cryptanalysis Methods

Exhaustive key search $\rightarrow$ Computing power, Moore's Law

Mathematical approaches $\rightarrow$ Creativity

Quantum computer

[under the cryptanalysis scenarios CO, KP, CP, CC, CT]

Exhaustive Key Search

- From the description of the algorithm, obtain the key size, key space, and the size of the key space (the total number of keys)
- Consider the scenarios: CO, KP, CP, CC, CT
- Write code and/or build a special-purpose computer
- Cost to build the (hw/sw) machine & time to obtain the key
- BIG QUESTION: Are there ciphers that cannot be cryptanalyzed with infinite amount of resources?

Mathematical Approaches

- Under the scenarios (CO, KP, CP, CC, CT), we consider how the plaintext or the key can be found using less resources (time/money) than the exhaustive search
- It seems that we would have a different approach for each cipher; However, there are classes of ciphers, requiring similar approaches
- Mathematically and algorithmically rich history
- Overnight fame is guaranteed if you "break" a commonly used cipher!
- Or: overnight riches ... with some possibility of jail time! :(

Quantum Computer

- A quantum computer is composed of
  1. A register containing of n qubits
  2. Multiqubit logic gates applied to the register according to an algorithm
  3. A measurement system determining the states of selected qubits at the end of computation
- Many problems in computer science are intractable on classical computers because there are too many possible inputs (or states)
- Due to superposition principle, a single quantum register is capable of simultaneously storing and processing all of the classical inputs at once
- A quantum computer is useful only if you have a quantum algorithm to solve a particular intractable problem

Quantum Computers and Cryptography

- Many public-key cryptographic algorithms (those relying on factorization problem and discrete logarithm problem) are breakable on a large enough quantum computer due to Shor's algorithm
- However, the research on quantum computer has not given us a reliable and large quantum computer (yet)
- There is a new body of research named **post-quantum cryptography** which refers to cryptographic algorithms that cannot (possibly) be broken on a quantum computer
- **Quantum cryptography** refers to research on using quantum mechanical techniques to achieve communication secrecy or quantum key distribution