Cryptography (and Information Security)
6CCS3CIS / 7CCSMCIS

Prof. Luca Viganò

Department of Informatics
King's College London, UK

First term 2020/21

Lecture 2.4: Cryptanalysis and brute-force attacks

Cryptanalysis and brute-force attacks

- Typical objective of attacking an encryption system
  - is not simply to recover the plaintext of a single ciphertext
  - but to recover the key in use (so that all future and past messages encrypted with that key are compromised).
- 2 general attack approaches:

Cryptanalysis

- Attacks rely on nature of the algorithm plus perhaps some knowledge of general characteristics of the plaintext or even some sample plaintext-ciphertext pairs.
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

Brute-force attack

- Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success.

Brute-force attack

- It is always possible: simply try every key until an intelligible translation of the ciphertext into plaintext is obtained.
  It thus assumes that plaintext is known or recognizable.
- Its cost (heavily) depends on key size and on average, half of all possible keys must be tried to achieve success.
- Average time required for exhaustive key search:

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu$s = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu$s = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu$s = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu$s = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu$s = 6.4×10^{12} years	6.4×10^6 years

  - Key size: 56 used for DES, 168 for triple DES, 128 (minimum size) for AES.
  - Also: substitution codes that use a 26-character key (discussed later), in which all possible permutations of the 26 characters serve as keys.
  - 1 decryption/μs is perfectly reasonable.
  - 10^6 decryption/μs (in the future?): DES no longer computationally secure!

Some comparisons for key size

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu$s = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu$s = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu$s = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu$s = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu$s = 6.4×10^{12} years	6.4×10^6 years

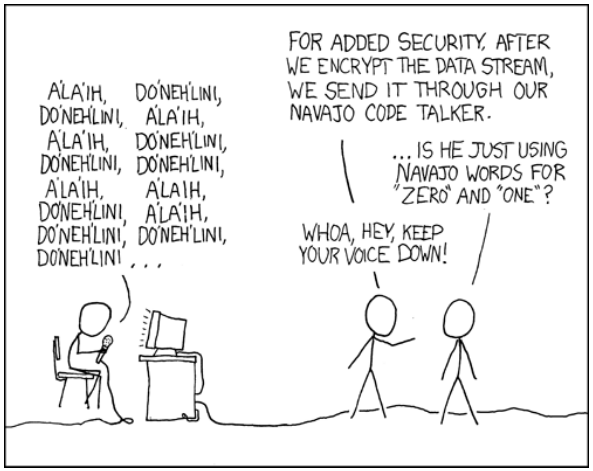
- 2^{92} atoms in the average human body
- 2^{128} possible keys for a 128-bit key (= total number of IP addresses available under IPv6)
- 2^{170} atoms in the planet
- 2^{233} atoms in the galaxy
- 2^{256} possible keys for a 256-bit key ($\approx 10^{77}$)

  10^{78} to 10^{82} atoms in the universe
- 2^{333} smallest power of 2 that is greater than googol (10^{100})

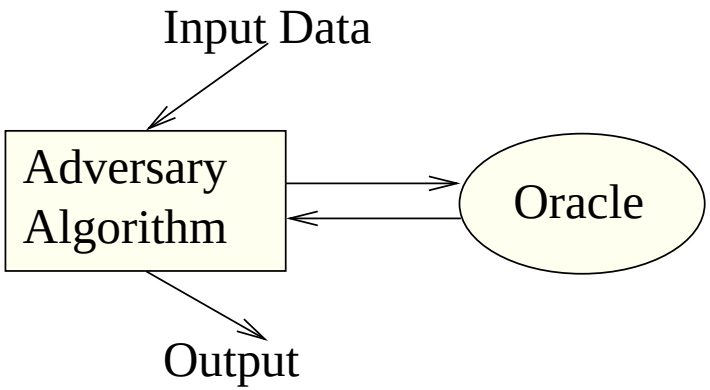
Cryptanalitic attacks

- Always assume attackers know the algorithms used!
  - Worst-case analysis and realistic in open systems.
  - Algorithms should be published to facilitate the evaluation of their security.
- Contrast with security by obscurity.

  Analogy: hide a letter under your mattress versus lock it in a safe, whose design has been published and whose locking mechanism has withstood attacks from the world's best safecrackers.
- But security by obscurity has proven extremely dangerous!



Model of Attack



We can think of the adversary as playing a game:

Input: Whatever adversary necessarily knows from the beginning, e.g., public key, distribution of plain texts, etc.

Oracle: Models information adversary can obtain during an attack. Different kinds of information characterize different types of attacks.

Output: Whatever the adversary wants to compute, e.g., secret key, partial information on plain text, etc. He wins if he succeeds.

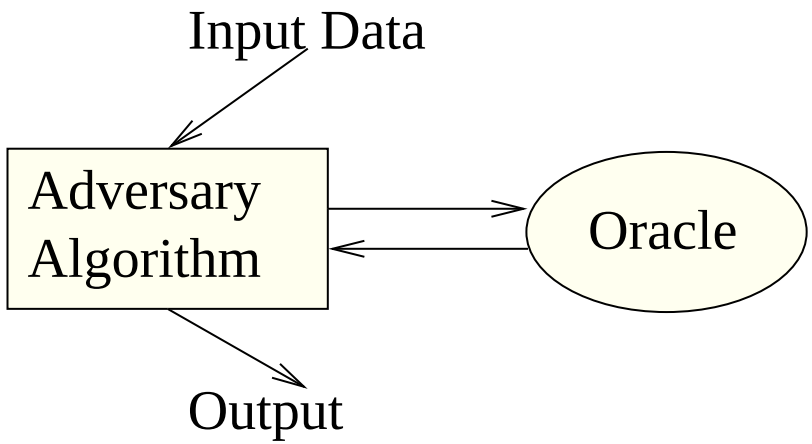
Types of attack

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Types of attack

- **Ciphertext only:**
  - **Given:** $C_1 = E_K(M_1), \ldots, C_n = E_K(M_n)$
  - **Deduce:** $M_1, \ldots, M_n$ or algorithm to compute M_{n+1} from $C_{n+1} = E_K(M_{n+1})$
- **Known plaintext:**
  - **Given:** $M_1, C_1 = E_K(M_1), \ldots, M_n, C_n = E_K(M_n)$
  - **Deduce:** Inverse key or algorithm to compute M_{n+1} from $C_{n+1} = E_K(M_{n+1})$
- **Chosen plaintext:** Same as above but cryptanalyst may choose $M_1, \ldots, M_n$.
- **Adaptive chosen plaintext:** Cryptanalyst can not only choose plaintext, but he can modify the plaintext based on encryption results.
- **Chosen ciphertext:** Cryptanalyst can chose different ciphertexts to be decrypted and gets access to the decrypted plaintext.

How to build a definition of security



1. Specify an oracle (a type of attack).
2. Define what the adversary needs to do to win the game, i.e., a condition on his output.
3. The system is secure under the definition, if any efficient adversary wins the game with only negligible probability.

A standard definition (conventional encryption)

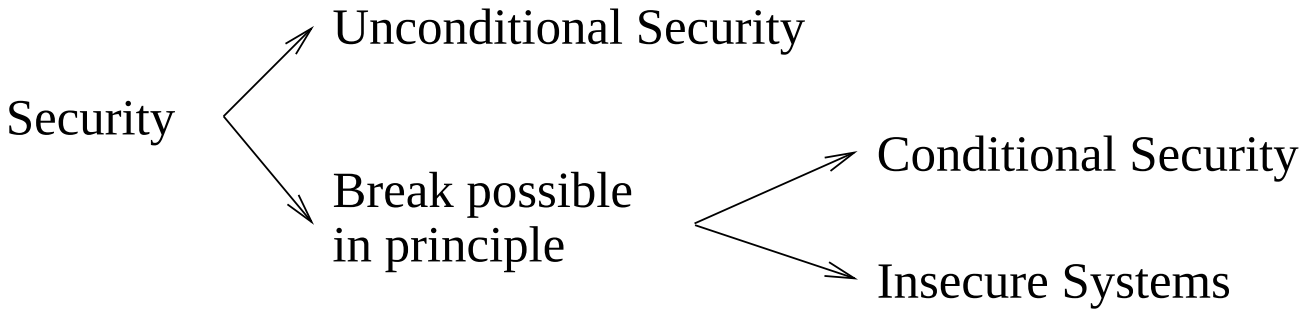
- No input data for adversary.
- Choose plaintext attack of following kind:

  Case 0: when asked to encrypt message m, oracle returns encryption of m under a fixed key that is randomly chosen initially; or

  Case 1: oracle returns encryption of a randomly chosen message, totally independent of m.

Idea: In case 1, adversary gets completely useless data. If he cannot tell this apart from correct encryptions, he cannot do any damage in the real world (case 0) either.

Classification of security



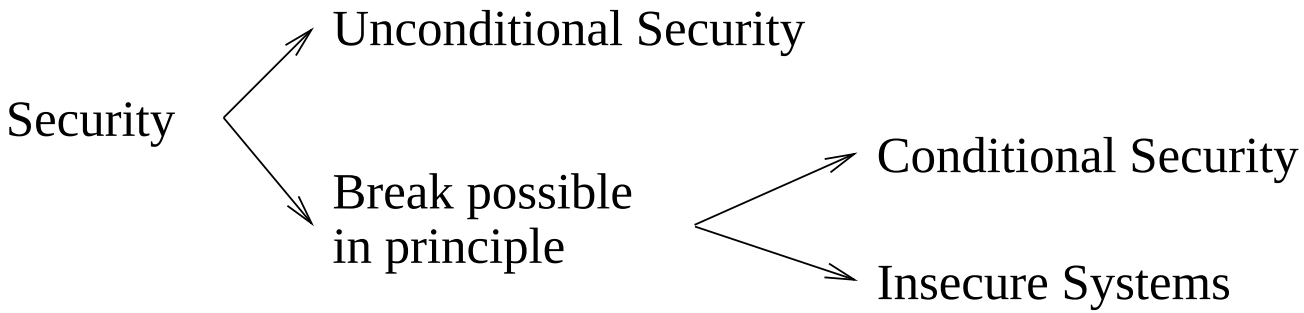
Unconditional Security

System (algorithm) is secure even if attacker has unbounded computing power since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext.

- Security measured using information theory.
- With exception of one-time pad, there's no unconditionally secure encryption algorithm.
- Hence, strive for algorithm that meets one or both of:
  - Cost of breaking cipher exceeds value of encrypted information.
  - Time required to break cipher exceeds useful lifetime of information.

Algo is **computationally secure** if either of these two criteria met.

Classification of security



Conditional Security

System can be broken in principle, but this requires more computing power than a realistic attacker would have.

- Security measured using complexity theory.

Reading

To know more, please read

- the subsection “Cryptanalysis and Brute-Force Attack” of chapter 3.1 in Stallings’ 2017 book (excerpt provided on KEATS),
- Section 1.13 (up until 1.13.3 included) in The Handbook of Applied Cryptography.

Reflect on your learning

- Have you achieved the learning outcomes for this week?
- This activity aims to help you to reflect and action plan to give you a live picture of your progress throughout the week and help you to identify your strengths and areas for development.
- Reflect on the questions asked in the next slide and answer them.
- You are encouraged to return to this activity after the live turorial(s) to see if your knowledge and understanding has progressed.

Reflect on your learning

	Not confident	Moderately confident	Very confident
Describe the motivation underlying cryptography and information security			
Describe basic terminology, concepts and notations of cryptography			
Explain the basic security properties, discussing how they can be achieved by means of cryptography			
Describe the basic cryptographic functions and provide a generic mathematical formalisation of cryptographic systems			
Explain symmetric-key encryption			