Lecture 1:
Course Introduction

Thomas Johansson

Course intro - Cryptography

- Welcome to Cryptography (EDIN01)!
- Everything in English!
- Course information
- The course web page: http://www.eit.lth.se

- Prerequisites: Math and programming skills!

Other crypto/security courses

- Dept. of EIT, Crypto and Security group
- (Continuation course for PhD students: Mathematical Cryptology (EDIN05), 7,5hp)
- Security courses:
  Computer Security (EIT060), 7,5hp
  Web Security (EITF05), 4hp
  Advanced Computer Security (EITN50) 7,5hp
  Advanced Web Security (EITN41), 7,5hp
  NEW COURSE: Secure Systems Engineering, 7.5hp (vt1 2020)
- Project in EIT (EITN35), 7,5hp
- Master's thesis: see the department website: http://www.eit.lth.se

Introduction to Cryptography

Much of the theoretical work in cryptography concerns *cryptographic primitives*, algorithms with basic cryptographic properties.

A *cryptographic protocol* involve back and forth communication among two or more parties.

- *Symmetric-key cryptography* – methods in which both the sender and receiver share the same key (block ciphers, stream ciphers, MAC algorithms).
- Cryptographic hash functions are a related and important class of cryptographic algorithms.
- *Public-key cryptography* – two different but mathematically related keys are used a public key and a private key.

History of cryptography

- Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption)
- Encryption was used to (attempt) to ensure secrecy for spies, military, and diplomats.
- The field has expanded to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs and secure computation, ...

History of cryptography

- The earliest known use of cryptography is some carved ciphertext on stone in Egypt (ca 1900 BCE),
- Julius Caesar who is reported to have used an early substitution cipher.
- **Steganography** (i.e., hiding even the existence of a message so as to keep it confidential) was also first developed in ancient times. Modern examples of steganography include the use of invisible ink, microdots, and digital watermarks to conceal information.

History of cryptography

- Ciphertexts produced by classical ciphers (and some modern ones) always reveal statistical information about the plaintext, which can often be used to break them.
- After the discovery of *frequency analysis* in the 9th century, nearly all such ciphers became more or less readily breakable by any informed attacker. Such classical ciphers still enjoy popularity today, though mostly as puzzles (see cryptogram).
- Essentially all ciphers remained vulnerable to cryptanalysis using this technique until the development of the *polyalphabetic cipher* around the year 1467.

History of cryptography

- In the mid 1800s Babbage showed that polyalphabetic ciphers of this type remained partially vulnerable to extended frequency analysis techniques.
- It was finally explicitly recognized in the 19th century that secrecy of a cipher's algorithm is not a sensible nor practical safeguard of message security; in fact, it was further realized that any adequate cryptographic scheme (including ciphers) should remain secure even if the adversary fully understands the cipher algorithm itself.

History of cryptography

- Security of the key used should alone be sufficient for a good cipher to maintain confidentiality under an attack. This fundamental principle was first explicitly stated in 1883 by Auguste Kerckhoffs and is generally called *Kerckhoffs' principle*.

History of cryptography

- Various physical devices and aids have been used to assist with ciphers, e.g. cipher disks
- Many mechanical encryption/decryption devices were invented early in the 20th century, and several patented, among them *rotor machines* – famously including the **Enigma machine** used by the German government and military during World War II.
- These machines lead to an increase in cryptanalytic difficulty after WWI.

The Enigma

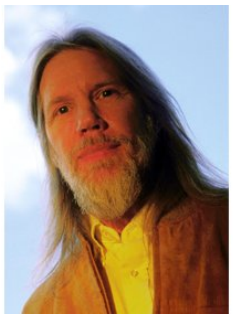
The Enigma machine, used, in several variants, by branches of the German military between the late 1920s and the end of World War II, implemented a complex electro-mechanical polyalphabetic cipher to protect sensitive communications. Breaking the Enigma cipher and the subsequent large-scale decryption of Enigma traffic at Bletchley Park, was an important factor contributing to the Allied victory in WWII.

The digital era

- The development of digital computers and electronics after WWII made possible much more complex ciphers.
- Computers allowed for the encryption of any kind of data representable in any binary format.
- Good modern ciphers have stayed ahead of cryptanalysis.
- Alternate methods of attack have become more attractive.

The birth of Public Key Cryptography

- Extensive open academic research into cryptography is relatively recent; it began only in the mid-1970s.
- Whitfield Diffie and Martin Hellman published their *key agreement algorithm* and the RSA algorithm was published shortly after. **Public key cryptography**




- Since then, cryptography has become a widely used tool in communications, computer networks, and computer security generally.

Modern cryptography

- Some modern cryptographic techniques can only keep their keys secret if certain mathematical problems are intractable, such as the *integer factorisation or the discrete logarithm problems*, so there are deep connections with abstract mathematics.
- There are no absolute proofs that a cryptographic technique is secure; at best, there are proofs that some techniques are secure if some computational problem is difficult to solve, and if assumptions about implementation or practical use are met.
- The potential effects of *quantum computing* are already being considered.

Modern cryptography

Symmetric-key cryptography

Block ciphers and stream ciphers, cryptographic hash functions and message authentication codes

Public-key cryptography

Public key encryption, digital signature schemes, key exchange protocols, electronic cash, interactive proof systems

Legal issues

- In some countries, even the domestic use of cryptography is, or has been, restricted. Until 1999, France significantly restricted the use of cryptography domestically, though it has relaxed many of these. In China, a license is still required to use cryptography.
- In the United States, cryptography is legal for domestic use, but there has been much conflict over legal issues related to cryptography. One particularly important issue has been the export of cryptography and cryptographic software and hardware.

Read more

Wikipedia

Simon Singh, *The Code Book*

David Kahn, *The Codebreakers - The Story of Secret Writing* (1967)