Code-Based Cryptography

Error-Correcting Codes and Cryptography



Code-Based Cryptography

- 1. Error-Correcting Codes and Cryptography
- 2. McEliece Cryptosystem
- 3. Message Attacks (ISD)
- 4. Key Attacks
- 5. Other Cryptographic Constructions Relying on Coding Theory

1. Error-Correcting Codes and Cryptography

- 1. Introduction I Cryptography
- 2. Introduction II Coding Theory
- 3. Encoding (Linear Transformation)
- 4. Parity Checking
- 5. Error Correcting Capacity
- 6. Decoding (A Difficult Problem)
- 7. Reed-Solomon Codes
- 8. Goppa Codes
- 9. McEliece Cryptosystem







































Enigma Machine

Private Key Cryptography

Popular Private-Key methods are: RC2, RC4, DES, 3DES, AES, ...



Public Key Cryptography

644

6

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEI

Abstract—Two kinds of contemporary developments in cryptography are examined. Witening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

I. INTRODUCTION

W ESTAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels of supply the equivalent of a written signature. At the me time, theoretical developments in information theory The best known cryptographi vacy: preventing the unauthorize tion from communications over order to use cryptography to insu

currently necessary for the communicating partness to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section 111 proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a public key cryptosystem enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering



Public Key Cryptography



Given *p*, *q* prime numbers EASY Compute N = p * q





The security of the **RSA** public-key cryptosystem relies on the **integer factorization**



The security of the **RSA** public-key cryptosystem relies on the **integer factorization**

Record Setting Calculation

The 768-bit RSA by the Number Field Sieve method (NFS) takes 2000 years (parallel computation)!

Trapdoor one-way functions - Discrete Logarithm

Given a group G and a generator g

Given x
$$\xrightarrow{\text{EASY}}$$
 Compute $h = g^x \mod p$

Trapdoor one-way functions - Discrete LogarithmGiven a group G and a generator gEASYComputeGiven xEASYCompute $h = g^x \mod p$ Find x such that
 $g^x = h \mod p$ Given hGiven h

Trapdoor one-way functions - Discrete LogarithmGiven a group G and a generator gGiven xFind x such that $g^x = h \mod p$ Given h

The security of the **DSA**, **Diffie-Hellman Key Exchange** and **ElGamal** public-key cryptosystem depend on the **DL problem**

Trapdoor one-way functions - Discrete Logarithm Given a group *G* and a generator *g*



The security of the **DSA**, **Diffie-Hellman Key Exchange** and **ElGamal** public-key cryptosystem depend on the **DL problem**

New Improvements in 2013

Quasi-polynomial algorithm for the **DL problem** in finite fields of small characteristic.

R. Barbulescu, P. Gaudry, A. Joux, E. Thomé.

A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. Advances in Cryptology - EUROCRYPT 2014, LNCS, volume 8441, pp.1-16, 2014.

Public Key Cryptography



Preparing for the Cryptopocalypse

Most PKC are based on INTEGER FACTORIZATION or the DLP

Preparing for the Cryptopocalypse Most PKC are based on INTEGER FACTORIZATION or the DLP Both can be attacked in polynomial time using Shor's → algorithm Quantum computer ECDSA RSA ECC USA HECC

Preparing for the Cryptopocalypse Most PKC are based on INTEGER FACTORIZATION or the DLP Both can be attacked in polynomial time using Shor's algorithm Quantum computer ECDSA RSA ECC -JSA HECC

Code-based Cryptography is a powerful alternative

1. Error-Correcting Codes and Cryptography

- 1. Introduction I Cryptography
- 2. Introduction II Coding Theory
- 3. Encoding (Linear Transformation)
- 4. Parity Checking
- 5. Error Correcting Capacity
- 6. Decoding (A Difficult Problem)
- 7. Reed-Solomon Codes
- 8. Goppa Codes
- 9. McEliece Cryptosystem

Pictures Licenses

- p. 3: Scarab with Pseudo-text / this file was provided to Wikimedia Commons by the <u>Walters Art Museum</u> as part of a <u>cooperation project</u>. All artworks in the photographs are in <u>public domain</u> due to age. The photographs of two-dimensional objects are also in the public domain.
- p. 3: <u>Scytale Wikipédia</u> / Luringen / permission is granted to copy, distribute and/or modify this document under the terms of the <u>GNU Free Documentation License</u>, Version 1.2 or any later version published by the <u>Free Software Foundation</u>; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
- p. 4: Enigma Machine / Photograph by Rama, CC BY-SA 2.0 fr via Wikimedia Commons
- p. 6: Composite picture of public-key cryptography inventors Whitfield Diffie and Martin Hellman. By Mary Holzer - CC-BY.