Academisch Schrijven voor Informatici

Bram in ’t Zandt
s4470346

Academisch Schrijven voor Informatici 2016/2017

April 2017

Contents

1. 16 april 2017

1.1 Opdracht 2

Link:
https://people.csail.mit.edu/rivest/Rsapaper.pdf

1.2 Opdracht 3

Doelgroep
De doelgroep van dit artikel zijn mensen met een achtergrond in de wiskunde of de informatica. Dit blijkt uit het feit dat in de Introduction al wordt verwezen naar mensen die misschien zelf al kennis hebben van een cryptosysteem ('Readers familiar with [1] may wish to skip directly to Section V for a description of our method.'). Ook wordt in de Abstract al gebruik gemaakt van verschillende wiskundige notaties die niet begrijpbaar zijn voor een leek op het gebied van Informatica. Een voorbeeld hiervan is $\equiv$ en $\mod$.

Boodschap
De schrijvers willen de lezers een introductie geven over een methode om digitale handtekeningen te zetten en voor het opzetten van een Public-Key Cryptosysteem. Dit blijkt vrij duidelijk uit de titel en uit de asbtract, die een vergelijking geeft tussen traditionele post (zoals brieven) en e-mail.

Effectiviteit
Ik vind de samenvatting van het artikel erg duidelijk. De inleiding van het artikel is echter erg kort en geeft niet goed weer waar het hele artikel over zal gaan. Dit is echter wel duidelijk uit de samenvatting. De samenvatting geeft een goede vergelijking tussen traditionele communicatie en meer moderne communicatie zoals email. Deze vergelijking wekt de interesse van de lezer om verder te lezen. De lezer weet namelijk waar het artikel over gaat.

A. **Paper**

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
2. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.

A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q. Decryption is similar; only a different, secret, power d is used, where $e \cdot d \equiv 1 \pmod{(p-1)\cdot(q-1)}$. The security of the system rests in part on the difficulty of factoring the published divisor, n.

Key Words and Phrases: digital signatures, public-key cryptosystems, privacy, authentication, security, factorization, prime number, electronic mail, message-passing, electronic funds transfer, cryptography.

CR Categories: 2.12, 3.15, 3.50, 3.81, 5.25

This research was supported by National Science Foundation grant MCS76-14294, and the Office of Naval Research grant number N00014-67-A-0204-0063.

Author's Address: Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139 E-mail addresses: rivest@theory.lcs.mit.edu

I Introduction

The era of "electronic mail" [10] may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved: (a) messages are *private*, and (b) messages can be *signed*. We demonstrate in this paper how to build these capabilities into an electronic mail system.

At the heart of our proposal is a new encryption method. This method provides an implementation of a "public-key cryptosystem," an elegant concept invented by Diffie and Hellman [1]. Their article motivated our research, since they presented the concept but not any practical implementation of such a system. Readers familiar with [1] may wish to skip directly to Section V for a description of our method.

II Public-Key Cryptosystems

In a "public key cryptosystem" each user places in a public file an encryption procedure E. That is, the public file is a directory giving the encryption procedure of each user. The user keeps secret the details of his corresponding decryption procedure D. These procedures have the following four properties:

(a) Deciphering the enciphered form of a message M yields M. Formally,

$$D(E(M) = M. \tag{1}$$

(b) Both E and D are easy to compute.

(c) By publicly revealing E the user does not reveal an easy way to compute D. This means that in practice only he can decrypt messages encrypted with E, or compute D efficiently.

(d) If a message M is first deciphered and then enciphered, M is the result. Formally,

$$E(D(M) = M. \tag{2}$$

An encryption (or decryption) procedure typically consists of a *general method* and an *encryption key*. The general method, under control of the key, enciphers a message M to obtain the enciphered form of the message, called the *ciphertext* C. Everyone can use the same general method; the security of a given procedure will rest on the security of the key. Revealing an encryption algorithm then means revealing the key.

When the user reveals E he reveals a very *inefficient* method of computing $D(C)$: testing all possible messages M until one such that $E(M) = C$ is found. If property (c) is satisfied the number of such messages to test will be so large that this approach is impractical.

A function E satisfying (a)-(c) is a "trap-door one-way function;" if it also satisfies (d) it is a "trap-door one-way permutation." Diffie and Hellman [1] introduced the