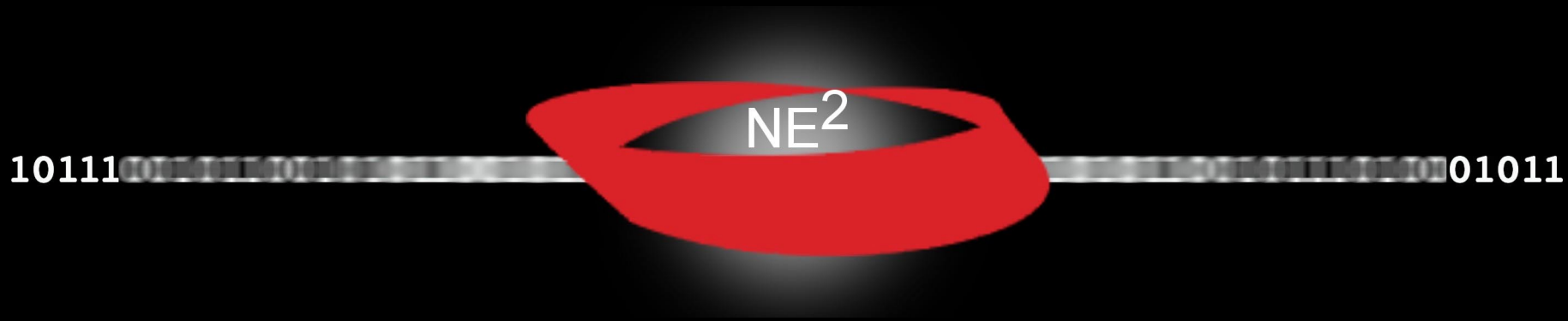


Encryption Providing Perfect Secrecy

NON-ELEPHANT
Encryption Systems Inc. (NE2)

An Overview of Encryption Methods

Presented at

Calgary Unix Users Group.

November 27, 2001

by: Mario Forcinito, PEng, PhD

With many thanks to Prof. Aiden Bruen from the Mathematics Department, University of Calgary, for his comments and invaluable help.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Introduction

The area of cryptography and privacy continues to expand.

On the commercial side, the projected size for the industry in the year 2004 was estimated by Lehman Brothers as being in the area of 13 billion dollars (as per their March 2001 figures).

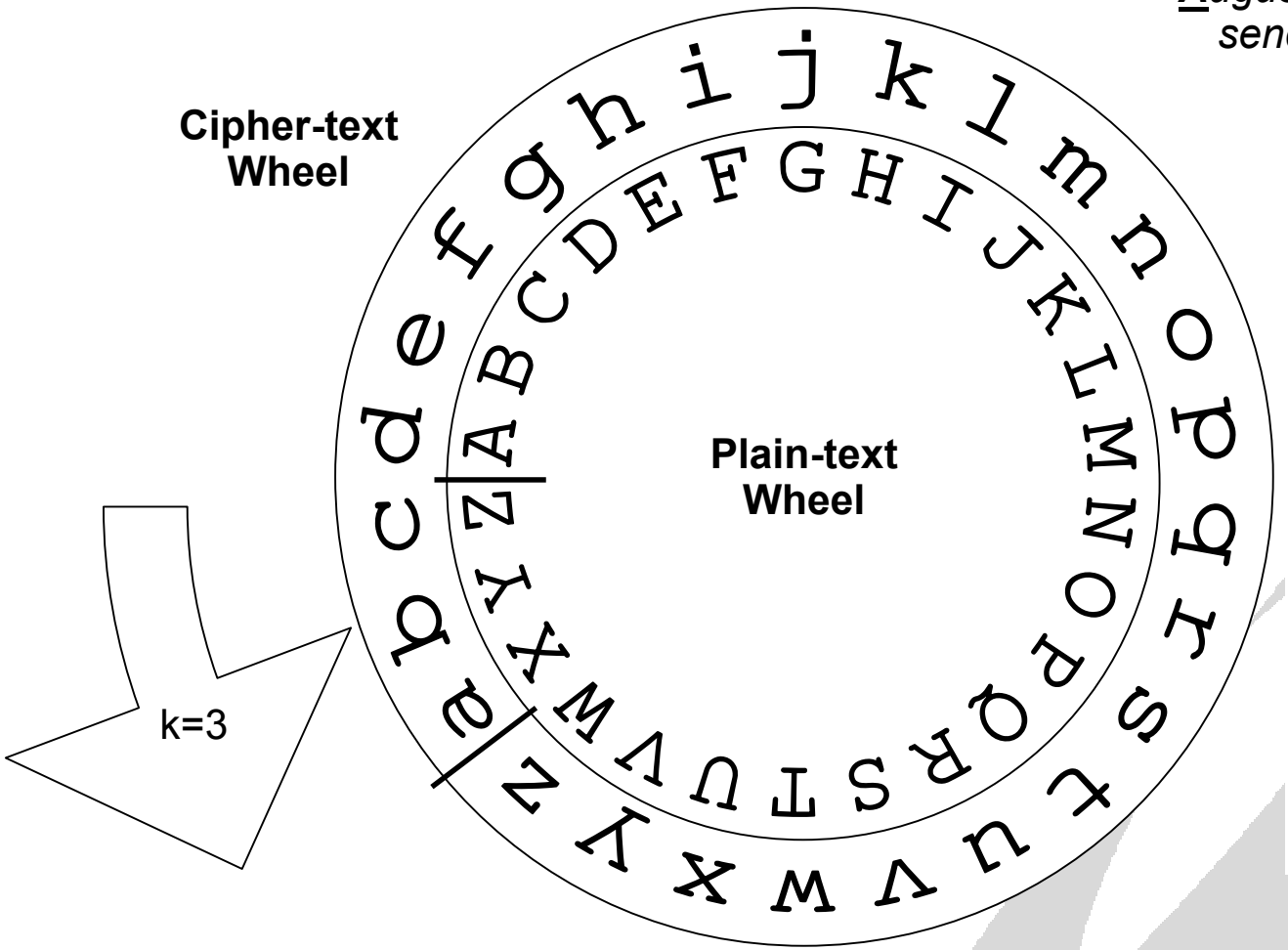
On the mathematical side, Universities continue to offer more and more courses in cryptography. Weightier and weightier tomes continue to be published. Obfuscation and prolixity are the order of the day. One is given the impression that the subject is a profound one, accessible only to experts.

In fact, the opposite is the case. There are only a few simple ideas needed. Nothing much has changed since the early days of cryptography in Ancient Greece and Rome. Indeed, it is my intention to cover ALL the main ideas in this lecture.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Cæsar Cipher

***A**ugustus Cæsar wants to send a **secret** message to **B**rutus*

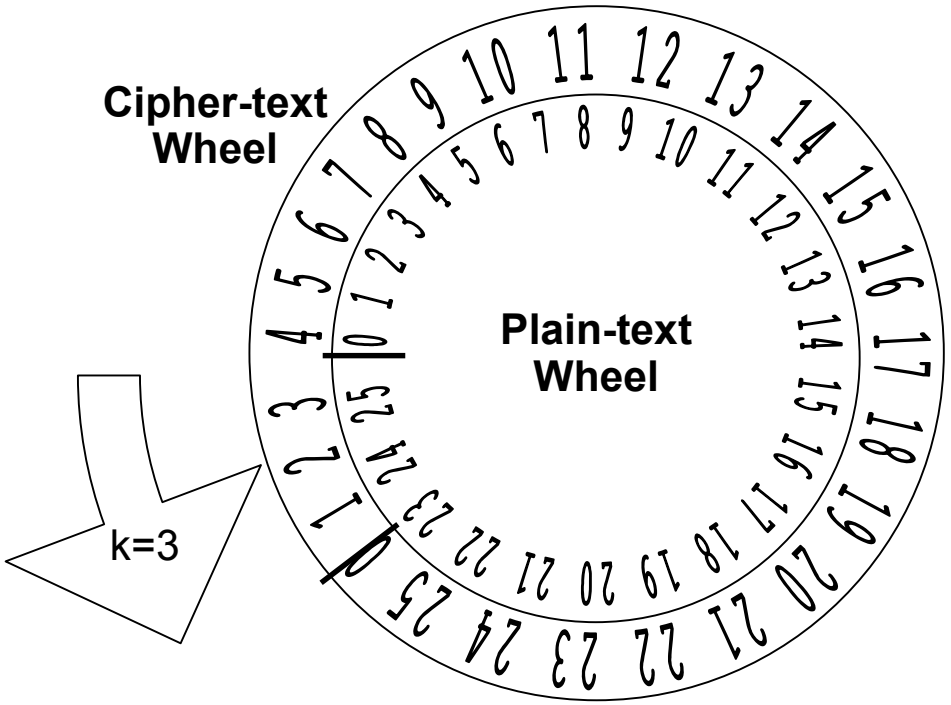


Example with k=3

Augustus enciphers (+ 3)
`SIX => vla`
and sends "`vla`"

Brutus receive "`vla`" and deciphers (- 3)
`vla => SIX`
because he knows that the session key is 3

Remarks



cipher = plain + 3

plain = cipher - 3

Works equally well if we use the numbers from 0 to 25 instead of the letters, and all the arithmetic is done modulo 26)

We perform modular arithmetic (modulo 12) every day.
If we start a task that takes us 4 hours at 10 A.M. we finish by 2 P.M. (instead of 14 A.M.) as 10 + 4 = 2 (mod 12)

The Cæsar cipher is the simplest example of a substitution cipher (it provides confusion).

Permutation of the characters in the text (after substitution) provides diffusion.

As pointed out by Shannon confusion and diffusion form the fundamental building blocks for ciphers.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Modern Ciphers

- Modern Ciphers work by combining complex confusion and diffusion techniques efficiently achieved only through computational (or mechanical) means.
- They still need a session key (or set of keys) to control the enciphering and deciphering processes. The key must remain secret.
- Ciphers that use the same key for encryption and decryption are called symmetric, e.g., DES.
- Well designed symmetric ciphers such as DES or AES are widely available and well-documented to be strong.
- Most problems arise from the the way in which keys are managed, stored , etc.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Perfect Secrecy
The One-Time Pad

A random binary sequence of the same length as the message can be used for encryption, e.g., if the session key is “101”

encipher: “6” =110 ⊕ 101 => 011

decipher: 011 ⊕ 101 => 110 = “6”

- A random binary sequence used in this way exemplifies Shannon’s definition of Perfect Secrecy and is called a **One-Time Pad**.
- Note that, in the Cæsar cipher, the methods for encryption and decryption are almost the same, i.e. rotate by +3 or –3, whilst in the one time pad the method for encryption and decryption is exactly the same, namely addition modulo 2

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Perfect Secrecy Remarks

- The one-time pad exemplifies unconditional security (“perfect secrecy”) in the sense of Shannon. There is no possible attack against unconditional security.
- Even machines with undreamed-of computing power will not be able to decipher the various Soviet spy messages encrypted with one-time pads during the cold war.

- **Utopia**

  Can one find an on-line method (as opposed to an off-line method) of generating a truly random key that can then be used as a one-time pad?

Catch 22

Catch 22 of Cryptography:

"Before Alice and Bob can communicate in secret, they must first communicate in secret."

S. Lomonaco, *A Quick Glance at Quantum Cryptography*,
1998 American Mathematical Society Lecture

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Key Exchange Methods Off-line

Off-Line | Mixed | On-line

Symmetric keys are exchanged through a secure, private channel (e.g. a courier).

This system is used frequently by the banking community.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Key Exchange Methods Mixed

Off-Line | Mixed | On-line

A trusted server generates and distributes the session keys. Each party has a secret key giving access to the server before the start. (Kerberos Model).

This method can also be used for Authentication

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Key Exchange Methods On-line

Off-Line | Mixed | On-line

A remarkable fact is that the session key can be generated in public (eavesdropping allowed) without any shared secret (= prior key). Examples of this are Public Cryptography, NE2 Cryptography.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

RSA Public Cryptography

- **B**ob selects: p, q and e (the encoding index)
  p, q: two distinct, secret primes;
  e: random integer having no common factors with $(p - 1).(q - 1)$.
- **B**ob calculates $N = p.q$ (the modulus), and d (the decoding index)
  from $e.d = 1 \pmod{(p - 1).(q - 1)}$
  e, N are made public (**B**ob's public key)
  p,q and d must remain secret (**B**ob's private key is d)
- **A**lice enciphers:=> $C = m^e \pmod{N}$ and send C to **B**ob
  Again, e is public and $C = m^e \pmod{N}$ is now public.

- **B**ob deciphers :=> $m = C^d \pmod{N}$ and recovers m
  (Think of m as a session key being transmitted)

NON-ELEPHANT
Encryption Systems Inc. (NE2)

RSA Public Cryptography

Strengths | Weaknesses

- Transfers a key on-line
- Based on sound mathematical results in number theory published in the late seventies
- Good market penetration
- Fairly well understood

NON-ELEPHANT
Encryption Systems Inc. (NE2)

RSA Public Cryptography

Strengths | Weaknesses

- If N can be factored then d, the secret key is easily calculated. Knowing d we can get the secret message
- Security rests on the assumption that the large integer (N) cannot be factored in a reasonable amount of time (i.e., offers only computational security)
- Vulnerable to attacks from quantum computers
- Long keys needed, very slow (see key length table below).
- Much pre-calculation needed for choosing appropriate p, q and e.
- The need for longer and longer keys makes RSA a somewhat decaying technology.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

NE2 Cryptography

Strengths | Weaknesses

- Constructs a random key on-line
- New technology
- Based on fundamental results -and their interconnections- in *Physics*, *Information Theory* and *Shannon Theory*, *Error-Correction Codes*, *Block Design* and *Classical Statistics*.
- Uses elegant mathematical work first published in the fifties.
- Invulnerable to attacks from quantum computers.
- No mathematical pre-calculations or expertise required.
- No key distribution, storage and maintenance cost.
- Small cryptographic foot-print and simple design.
- Very fast; over 1000 times faster than RSA. (ideally suited for WAPs)
- NE2 Cryptography represents the first practical realization of perfect secrecy systems theorized about by Shannon.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

NE2 Cryptography

Strengths | Weaknesses

- It is a new technology
- Has not yet achieved market penetration.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Utopia

Concerning our earlier question let us say this.

Utopia?
It seems yes.

Digital Signatures

Handwritten signatures have long been used as a proof of authorship. The idea can be extended to the digital world.

For example, for a symmetric cryptosystems with a trusted server **T** which has established secret keys K_A and K_B with **A** and **B** respectively, here is a simple way of implementing this.

- **A** encrypts her message m to **B** with K_A and sends it to **T**
- **T** decrypts m with the key K_A
- **T** takes the decrypted message and a statement that **T** has received this message from **A** and encrypts the whole bundle with K_B.
- **T** sends the encrypted bundle to **B.**
- **B** decrypts the bundle with K_B. **B** can now read both the message and the certification from **T** that **A** sent it.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Authentication

In any cryptosystem, when **A** is transmitting a message to **B**, there is the danger that an intruder (**Eve**) will intercept and modify, delete or generate messages. This is called the person-in-the-middle-attack. The attack can be nullified if **A, B** can verify that they are in fact, talking to each other and not to some imposter (e.g. suppose **A** is sending an encrypted message to **B** and **B** returns the decrypted message. **A** can only conclude that the object with whom **A** is communicating is in possession of **B**'s secret key: **A** cannot conclude the object is **B.**)

- With public key systems this authentication is done by means of digital certificates . In other words a trusted "Certificate Authority" certifies the identity of **A, B**. In theory, a Certificate Authority (CA) binds **B**'s secret key to the individual **B.**
- With symmetric key systems a Kerberos-style trusted server **T** (logically equivalent to a CA) performs the same function. This is the basis of the system being used by Windows 2000.
- NE2 protocol represents an improvement to this system whereby **T** controls the authentication for **A, B** but **T** is not privy to the messages.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Speed and Key Length Comparison

We conclude with some remarks on speed and key-length.

As regards speed, Prof. R.A. Mollin points out in his textbook that “For instance at its fastest, RSA is a roughly thousand times slower than DES”.

For the record, we enclose the information on comparative key-lengths between public and symmetric key cryptography.

Key lengths providing the same security

from *Applied Cryptography, 2nd Ed.*

by B Scheneier, John Wiley & Sons, 1996.

Symmetric key length	Public key length
56 bits	384 bits
64 bits	512 bits
80 bits	768 bits
112 bits	1792 bits
128 bits	2304 bits

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Summary

- We have covered ALL the main scientific points in cryptography.
- It is difficult to predict future scientific developments. Certainly, speed and security of keys will be essential.
- On the purely administrative and marketing side, different models of authentication (Kerberos, PKI, etc.) will continue to compete for market share.
- It seems completely unrealistic to assume that ANY one particular model will work best in ALL situations.
- Because of the strengths of the NE2 system and its quantum properties, we may well have reached the “end of the line” for key exchanges.

NON-ELEPHANT
Encryption Systems Inc. (NE2)

Contact NE2

Phone: (403) 232 6001
Fax: (403) 232 6017

400, 1010 - 8th Ave SW
Calgary AB Canada
T2P 1J2

http://www.ne2encryption.com/

Dr. Mario Forcinito
mario.forcinito@ne2encryption.com