FNNC ZESDQMNNM !

Sghr kdbstqd hr zants dmbqxoshnm

Outline

- Part 1: Cryptography, pre-1970
  - A lot of the history of pre-internet cryptography is relevant for today
- Part 2: Public-key cryptography
  - A major technological breakthrough
- Part 3: The crypto policy debate 1990-2000
  - A case study for policy stresses caused by technology

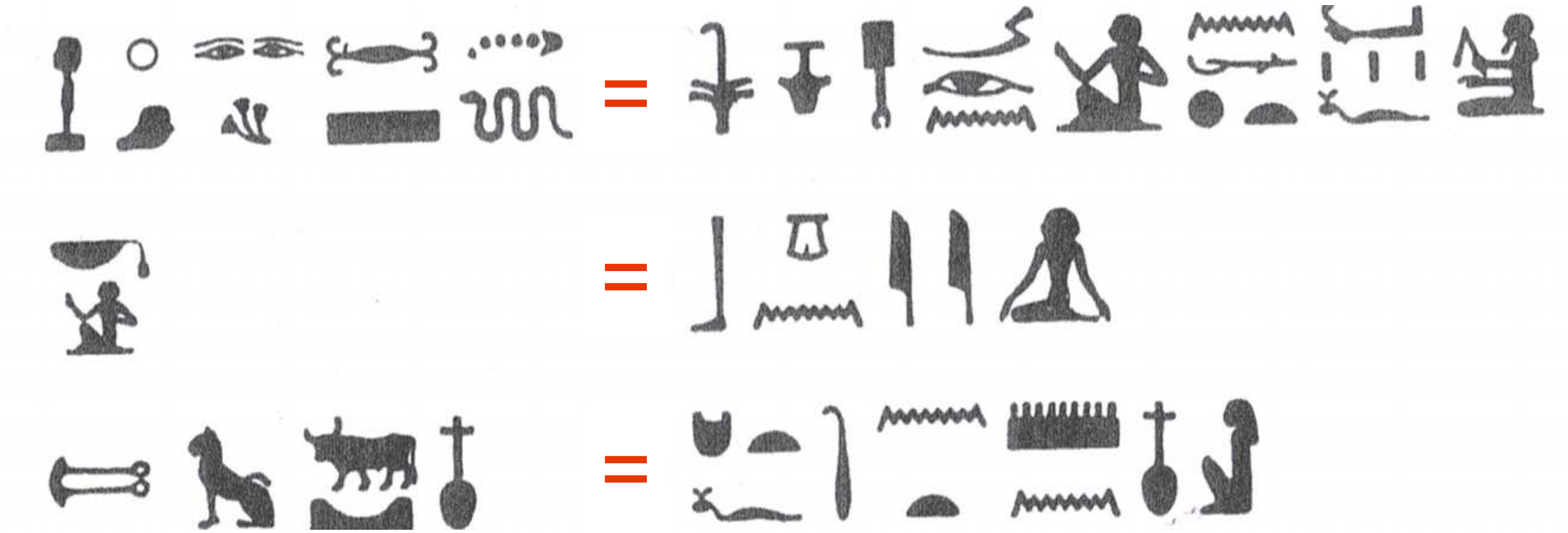
Security needs on networks

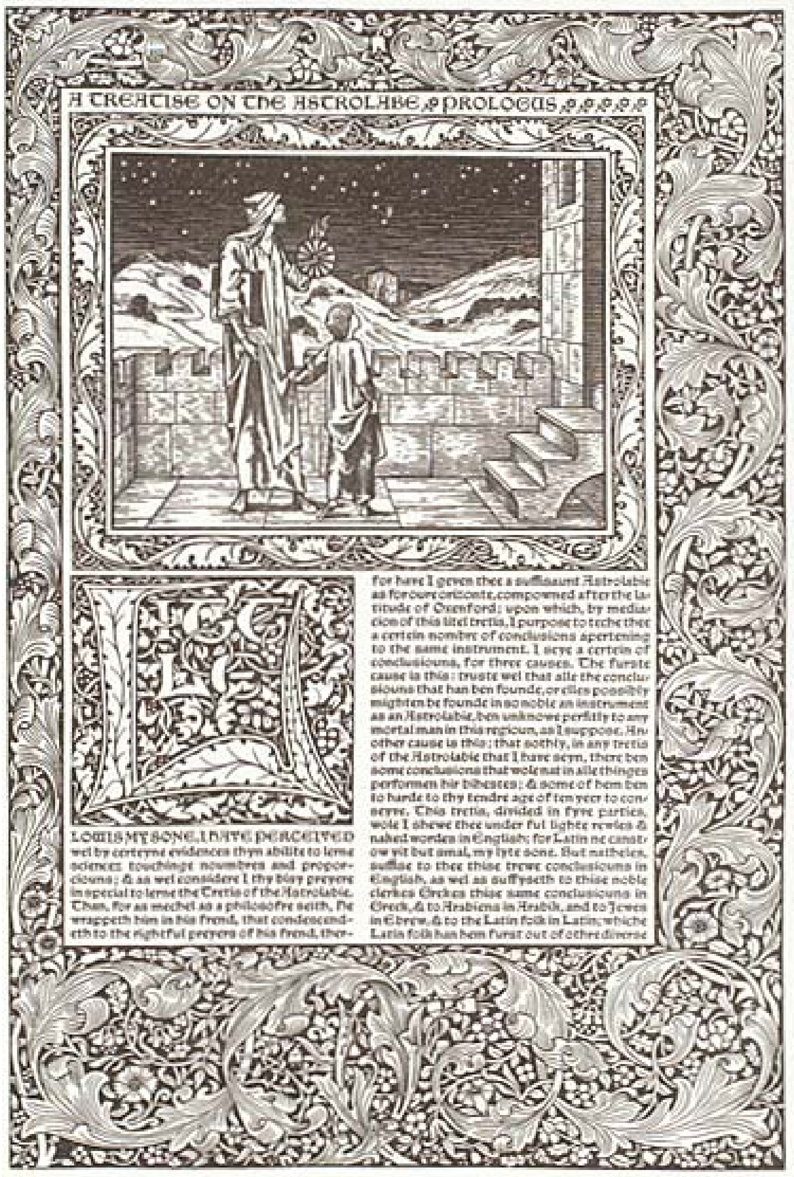
- **Confidentiality**: Only authorized people - e.g., the sender and recipient of a message, and not any eavesdroppers - can know the message.

Implemented using encryption

- **Authentication**: When Bob receives a message that purports to be sent by Alice, Bob can be sure that the message was really sent by Alice.
- **Integrity**: When Bob receives a message, he can be sure that it was not modified en route after Alice sent it.
- **Non-repudiation**: Alice cannot later deny that the message was sent. Bob cannot later deny that the message was received.

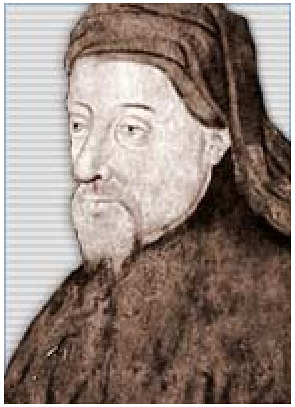
Cryptography, ca. 1900BC

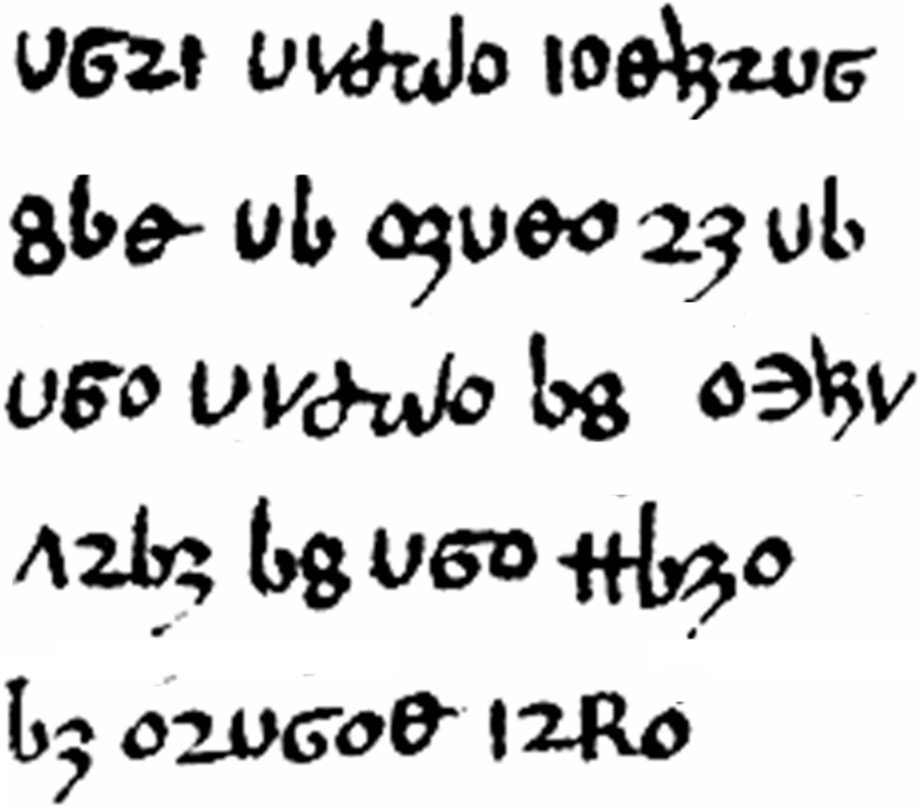




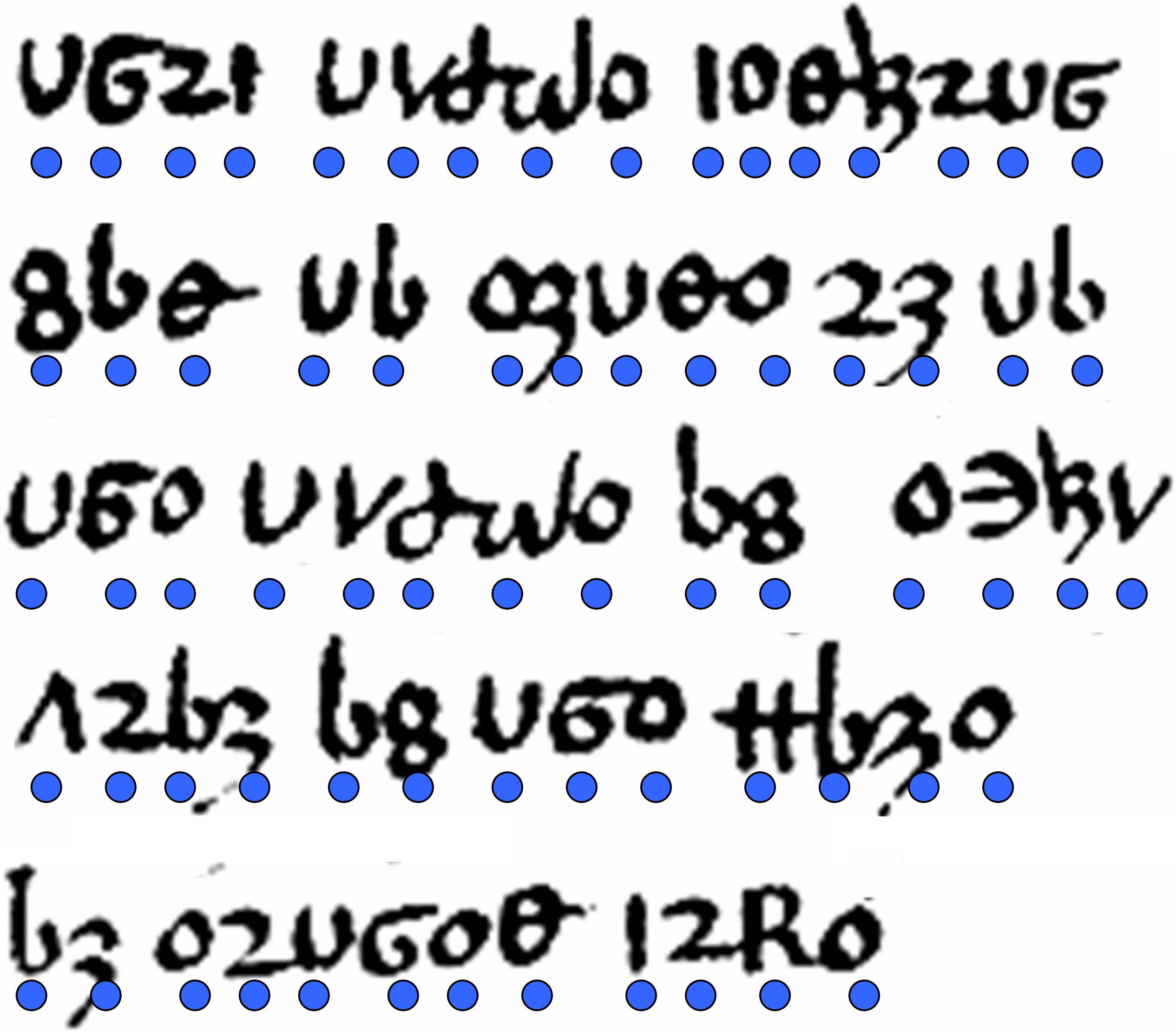
A TREATISE ON THE ASTROLABE. PROLOGUS.

LITEL LOWIS MY SONE, I HAVE PERCEIVED wel by certeyne evidences thyn abilite to lerne sciences touchinge noumbres and proporciouns; & as wel considere I thy bisy preyere in special to lerne the Tretis of the Astrolabie. Than, for as mechel as a philosofre seith, he wrappeth him in his frend, that condescendeth to the rightful preyers of his frend, therfor have I geven thee a suffisaunt Astrolabie as for oure orizonte, compowned after the latitude of Oxenford; upon which, by mediacioun of this litel tretis, I purpose to teche thee a certein nombre of conclusiouns apertening to the same instrument. I seye a certein of conclusiouns, for three causes. The furste cause is this: truste wel that alle the conclusiouns that han ben founde, or elles possibly mighten be founde in so noble an instrument as an Astrolabie, ben unknowe perfitly to any mortal man in this regioun, as I suppose. Another cause is this: that sothly, in any tretis of the Astrolabie that I have seyn, there ben some conclusiouns that wol nat in alle thinges performen hir bihestes; & some of hem ben to harde to thy tendre age of ten yeer to conseyve. This tretis, divided in fyve parties, wole I shewe thee under ful lighte rewles & naked wordes in English; for Latin ne canstow yit but smal, my lyte sone. But natheles, suffise to thee thise trewe conclusiouns in English, as wel as suffyseth to thise noble clerkes Grekes thise same conclusiouns in Greek, & to Arabiens in Arabik, and to Jewes in Ebrew, & to the Latin folk in Latin; whiche Latin folk han hem furst out of othre diverse

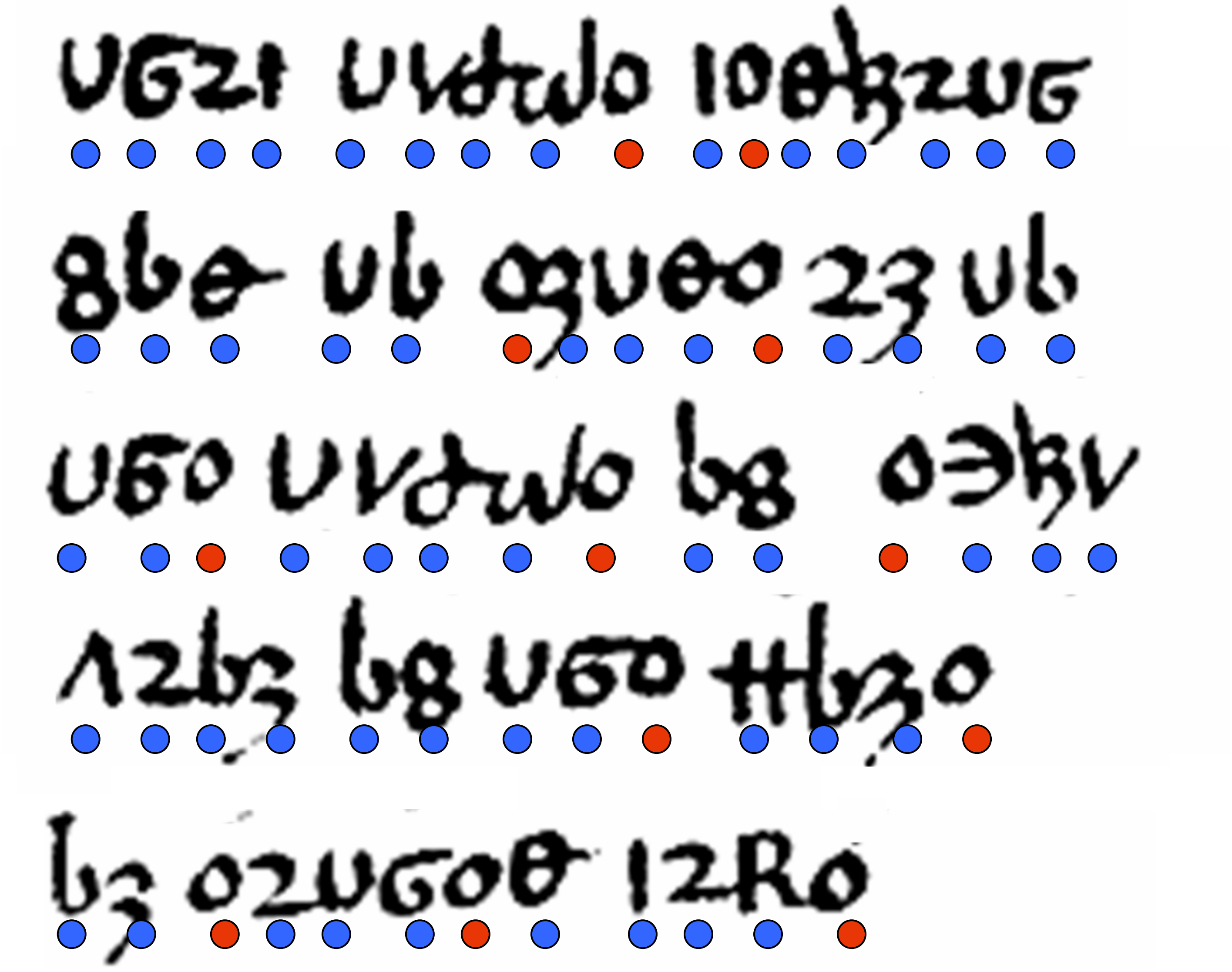




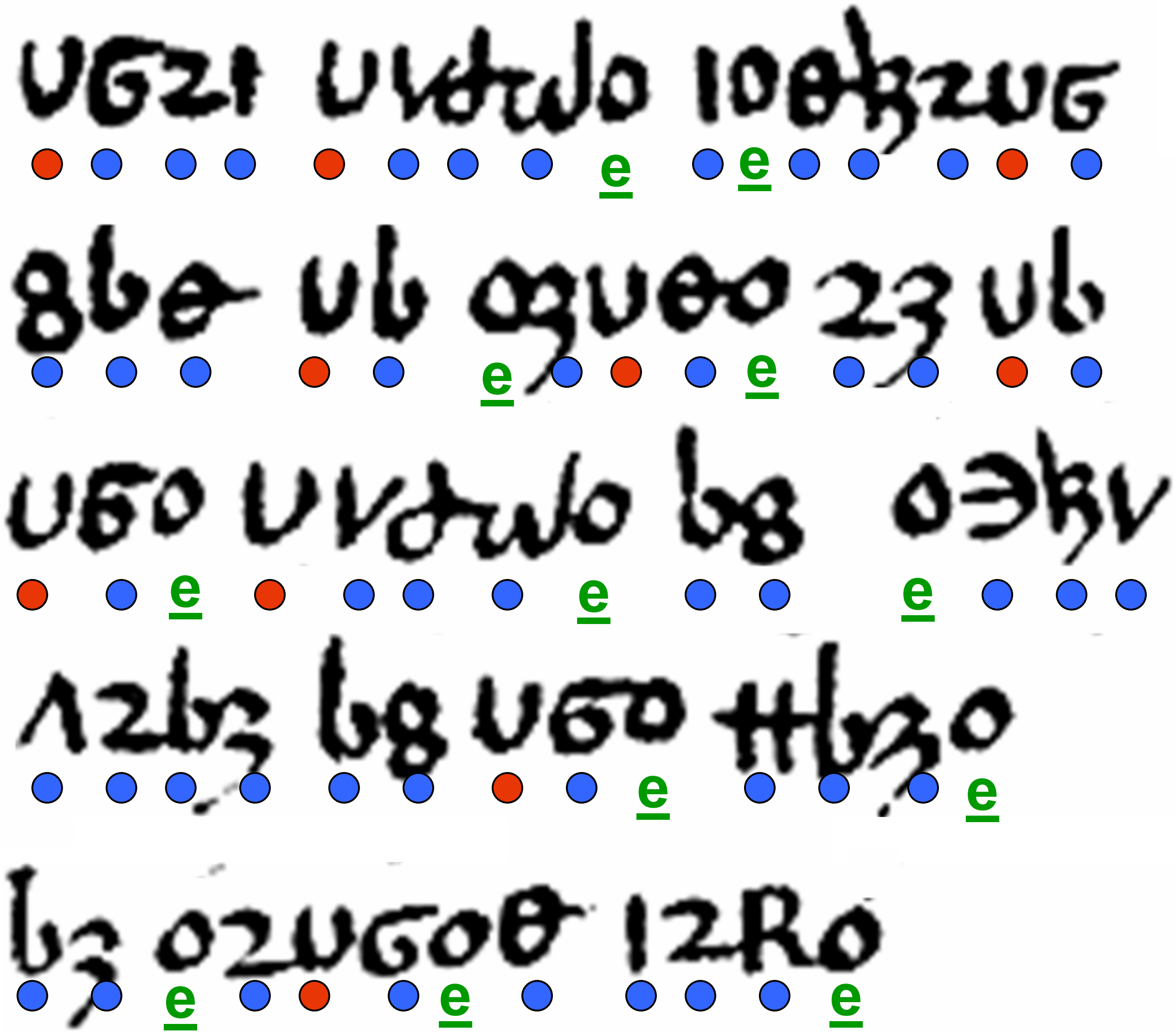
Geoffrey Chaucer, *Treatise on the Astrolabe,* 1391



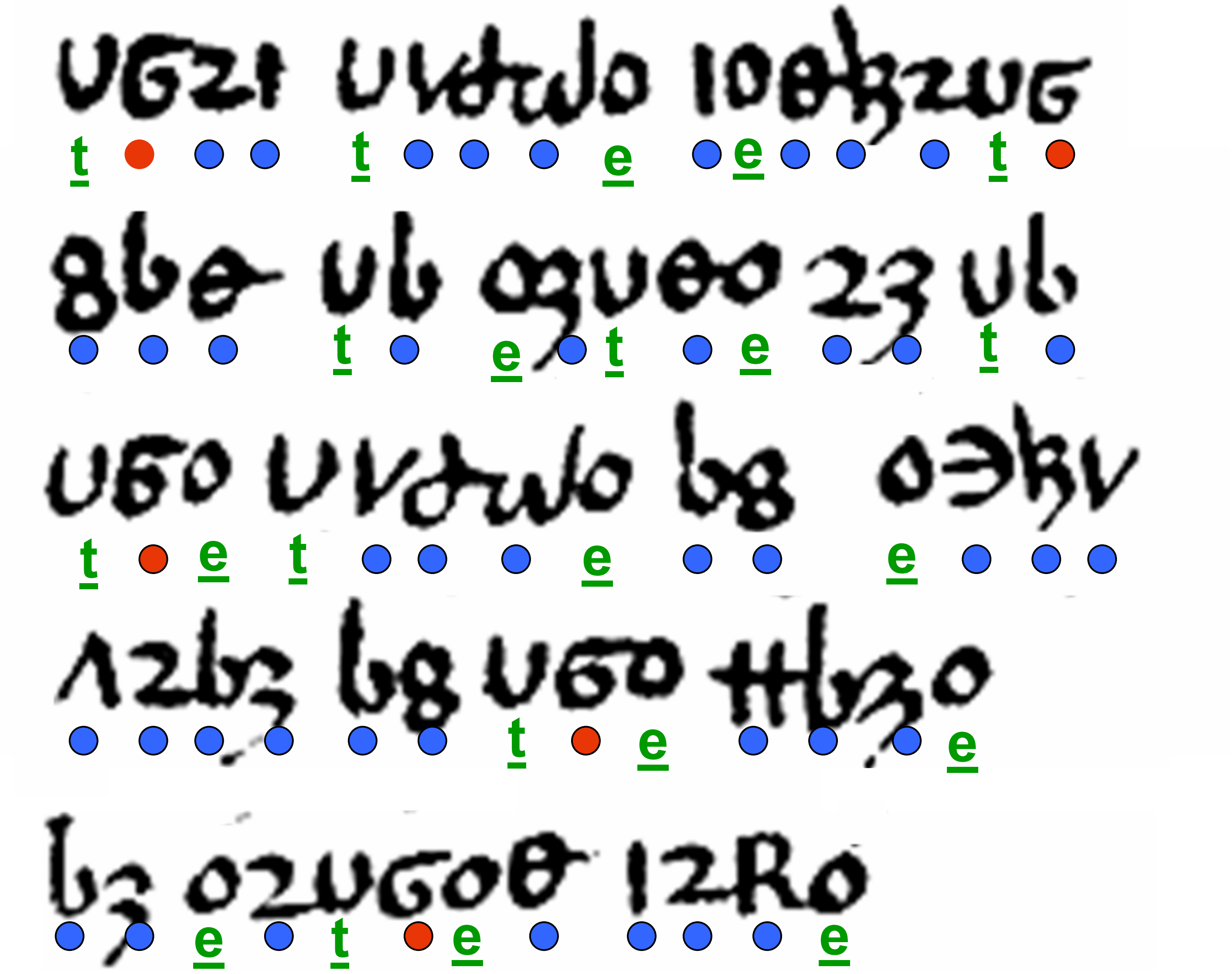
Geoffrey Chaucer, *Treatise on the Astrolabe,* 1391



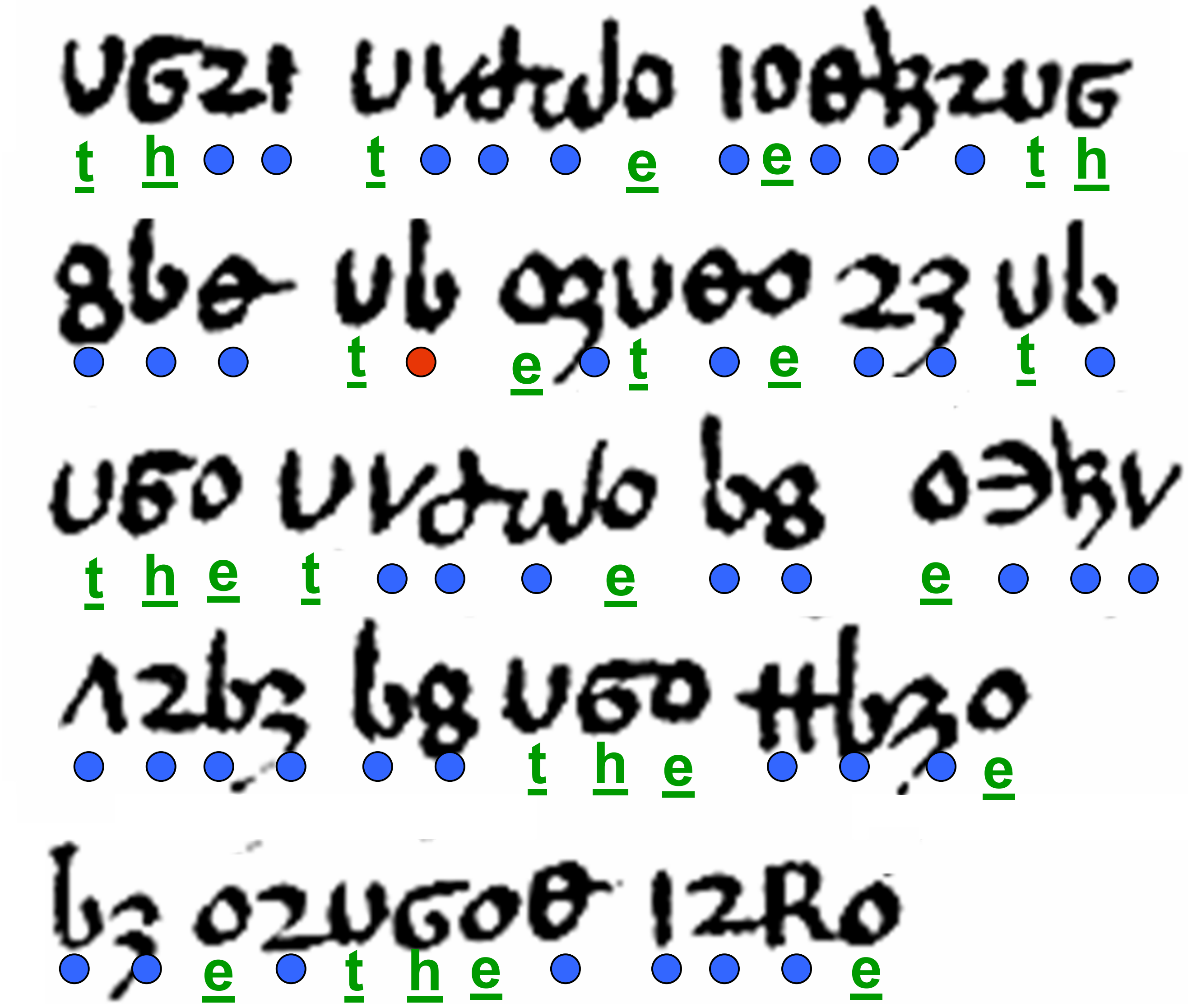
Geoffrey Chaucer, *Treatise on the Astrolabe,* 1391



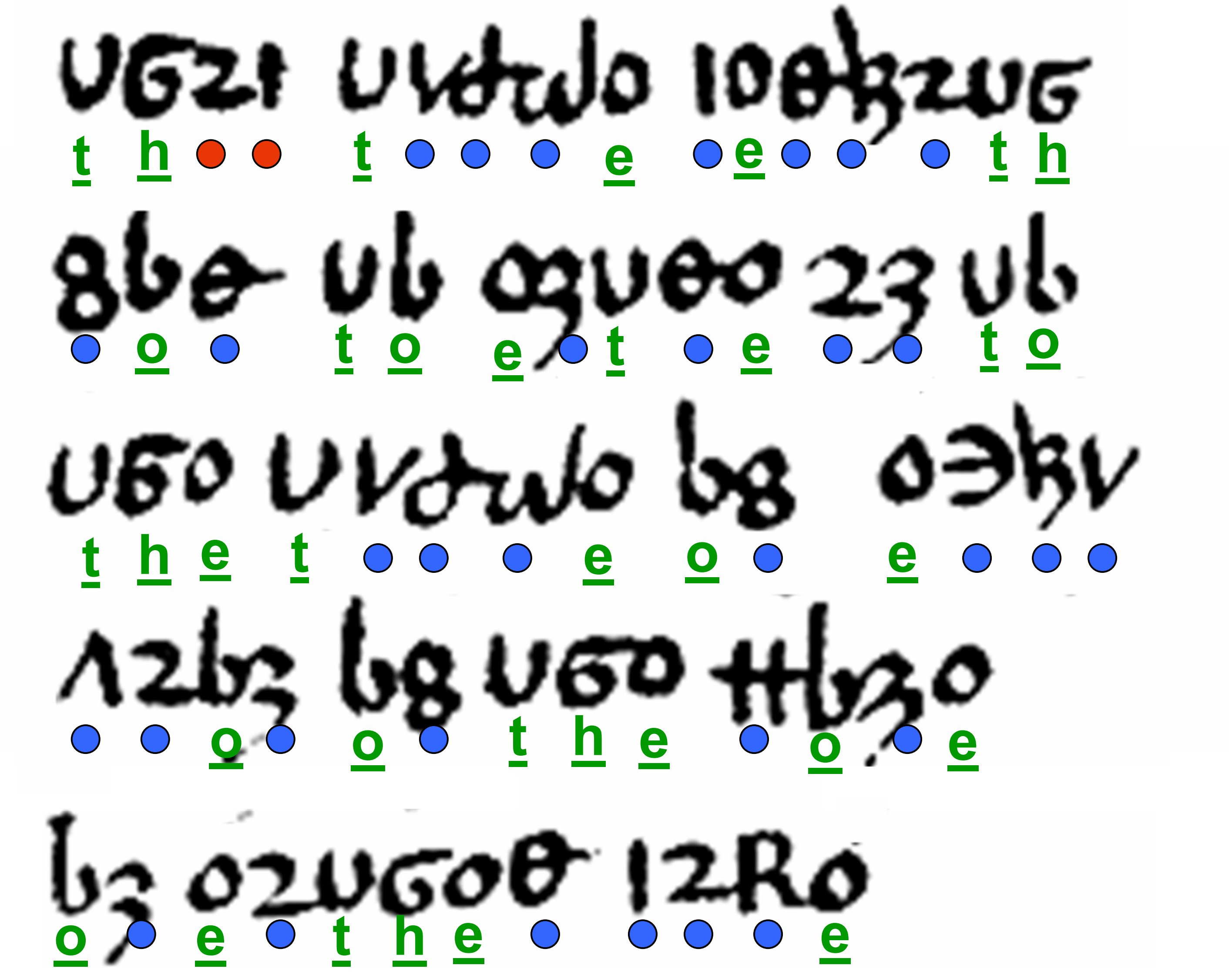
Geoffrey Chaucer, *Treatise on the Astrolabe*, 1391


t t e e t
t e t e t
t e t e e
t e e
e t e e

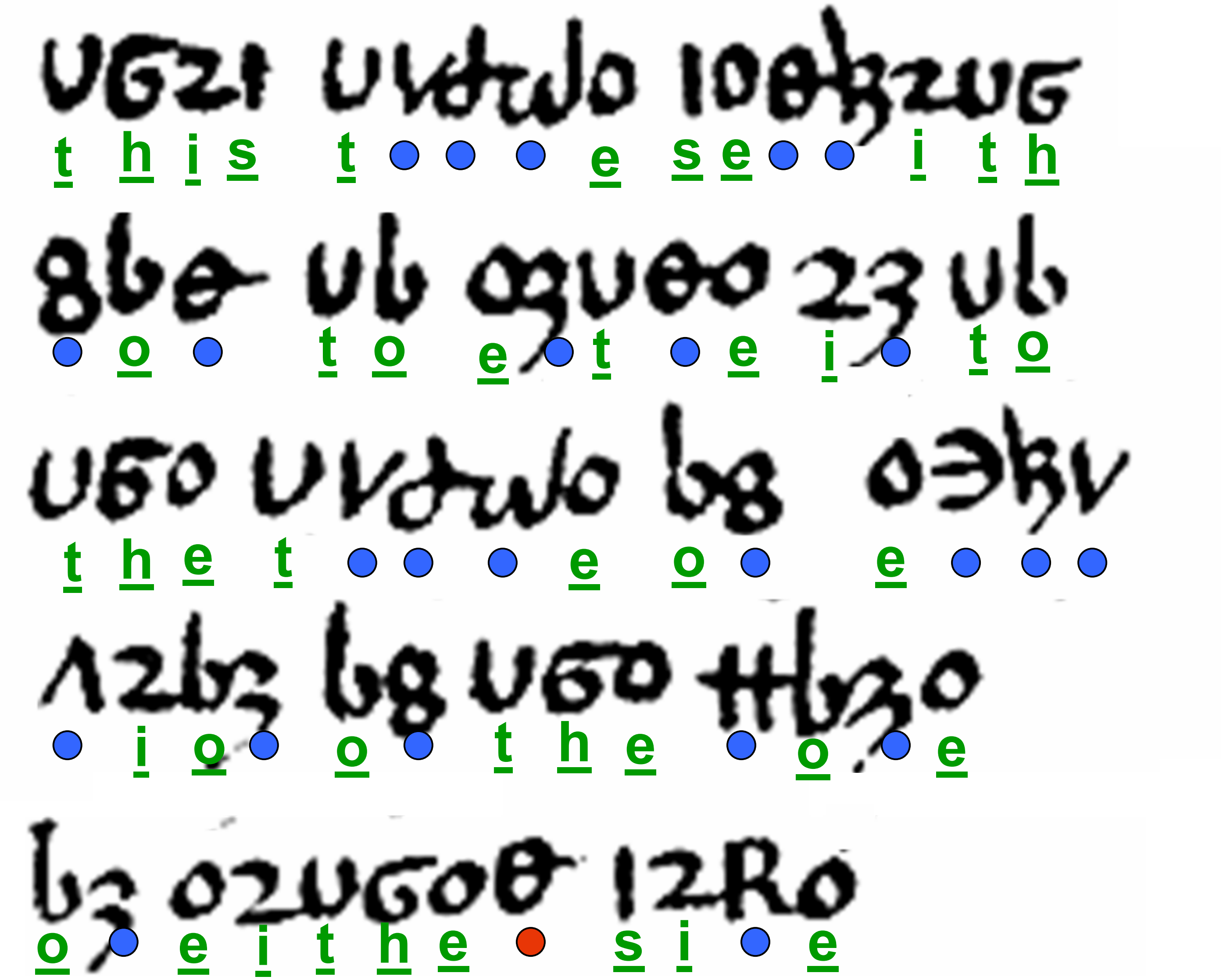
Geoffrey Chaucer, *Treatise on the Astrolabe*, 1391


t h ● ● t ● ● ● e ● e ● ● ● t h
● ● ● t ● e ● t ● e ● ● t ●
t h e t ● ● ● e ● ● e ● ● ●
● ● ● ● ● ● t h e ● ● ● e
● ● e ● t h e ● ● ● ● e

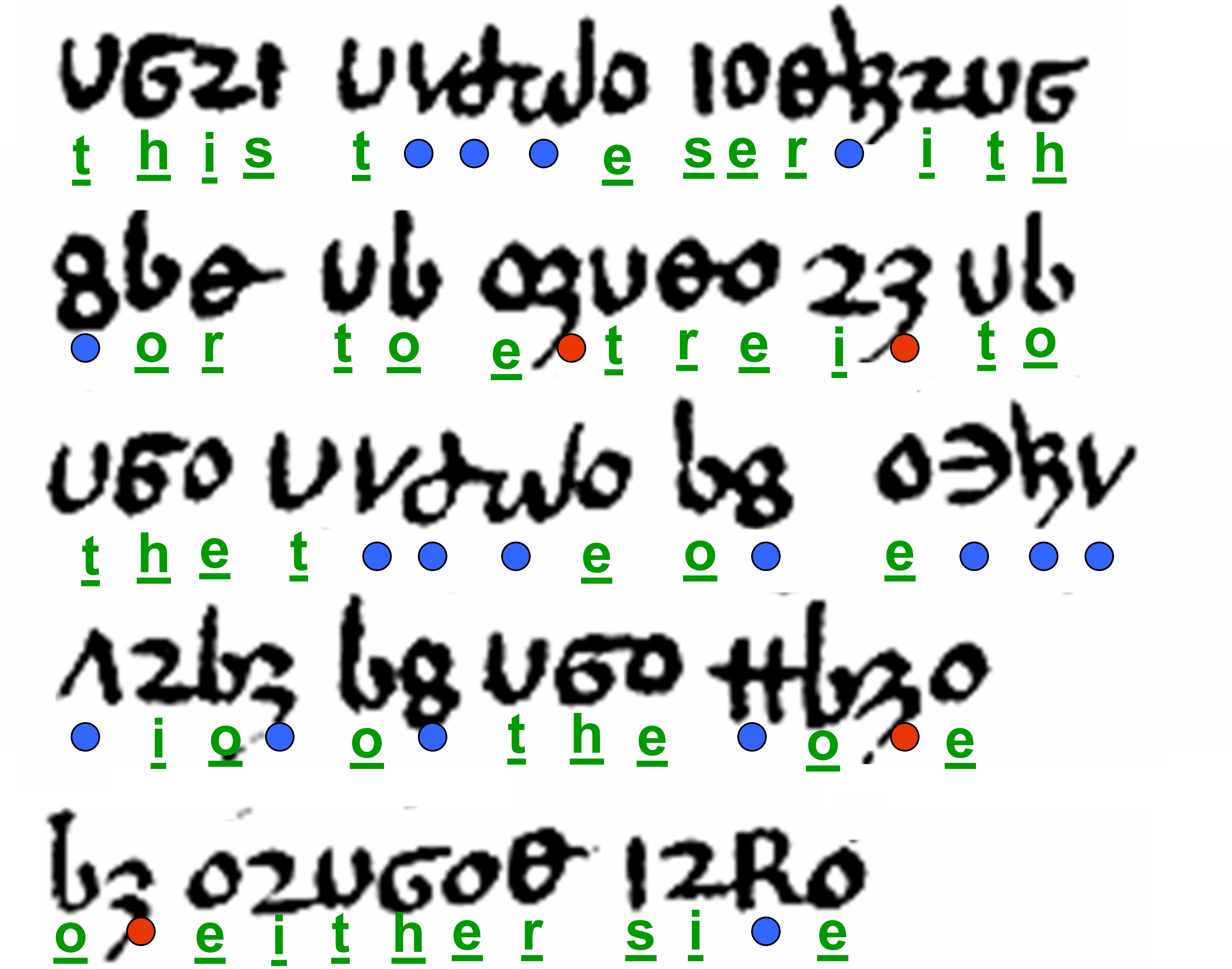
Geoffrey Chaucer, *Treatise on the Astrolabe,* 1391


t h ● ● t ● ● ● e ● e ● ● ● t h
● o ● t o e ● t ● e ● ● t o
t h e t ● ● ● e o ● e ● ● ●
● ● o ● o ● t h e ● o ● e
o ● e ● t h e ● ● ● ● e

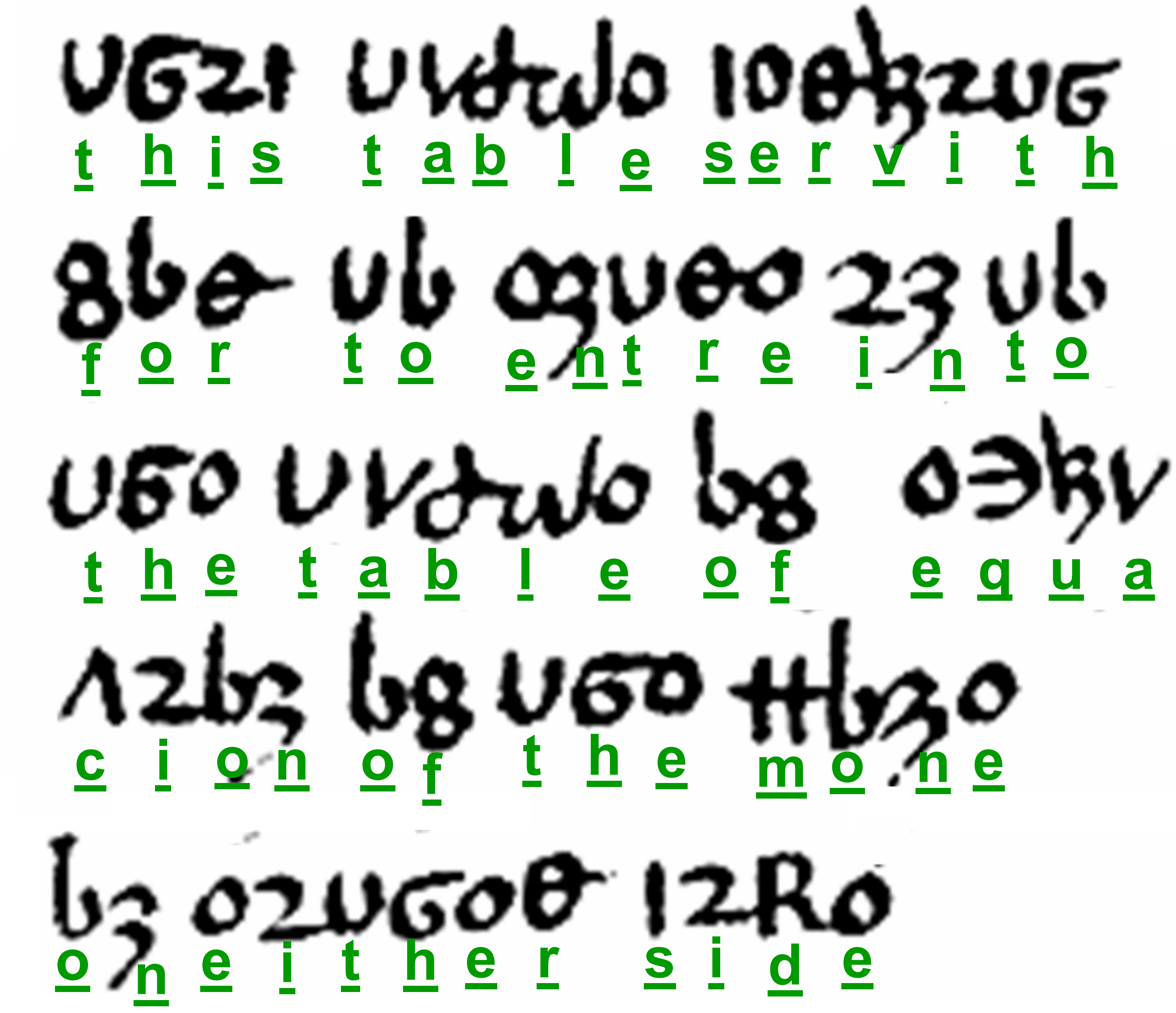
Geoffrey Chaucer, *Treatise on the Astrolabe*, 1391


t h i s t ● ● ● e s e ● ● i t h
● o ● t o e ● t ● e i ● t o
t h e t ● ● ● e o ● e ● ● ●
● i o ● o ● t h e ● o ● e
o ● e i t h e ● s i ● e

Geoffrey Chaucer, *Treatise on the Astrolabe*, 1391


t h i s t ● ● ● e s e r ● i t h
● o r t o e ● t r e i ● t o
t h e t ● ● ● e o ● e ● ● ●
● i o ● o ● t h e ● o ● e
o ● e i t h e r s i ● e

Geoffrey Chaucer, *Treatise on the Astrolabe,* 1391



this table servith
for to entre into
the table of equa
cion of the mone
on either side

Geoffrey Chaucer, *Treatise on the Astrolabe,* 1391

Substitution cipher

- Replace each character of the message by another character, according to some rule
- *Simple* or *monoalphabetic* substitution: All occurrences of a given character in the message are replaced by the same character
- In general
  - Original message is called the *plaintext*
  - Encrypted result is called the *ciphertext*

Caesar cipher

- Replace each letter by the letter that comes some fixed distance before or after it in the alphabet.

Shift = 3

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Omnia Gallia in tres partes divisa est

LJKF XDXI IFXF KQOB PMXO QBPA FSFP XBPQ

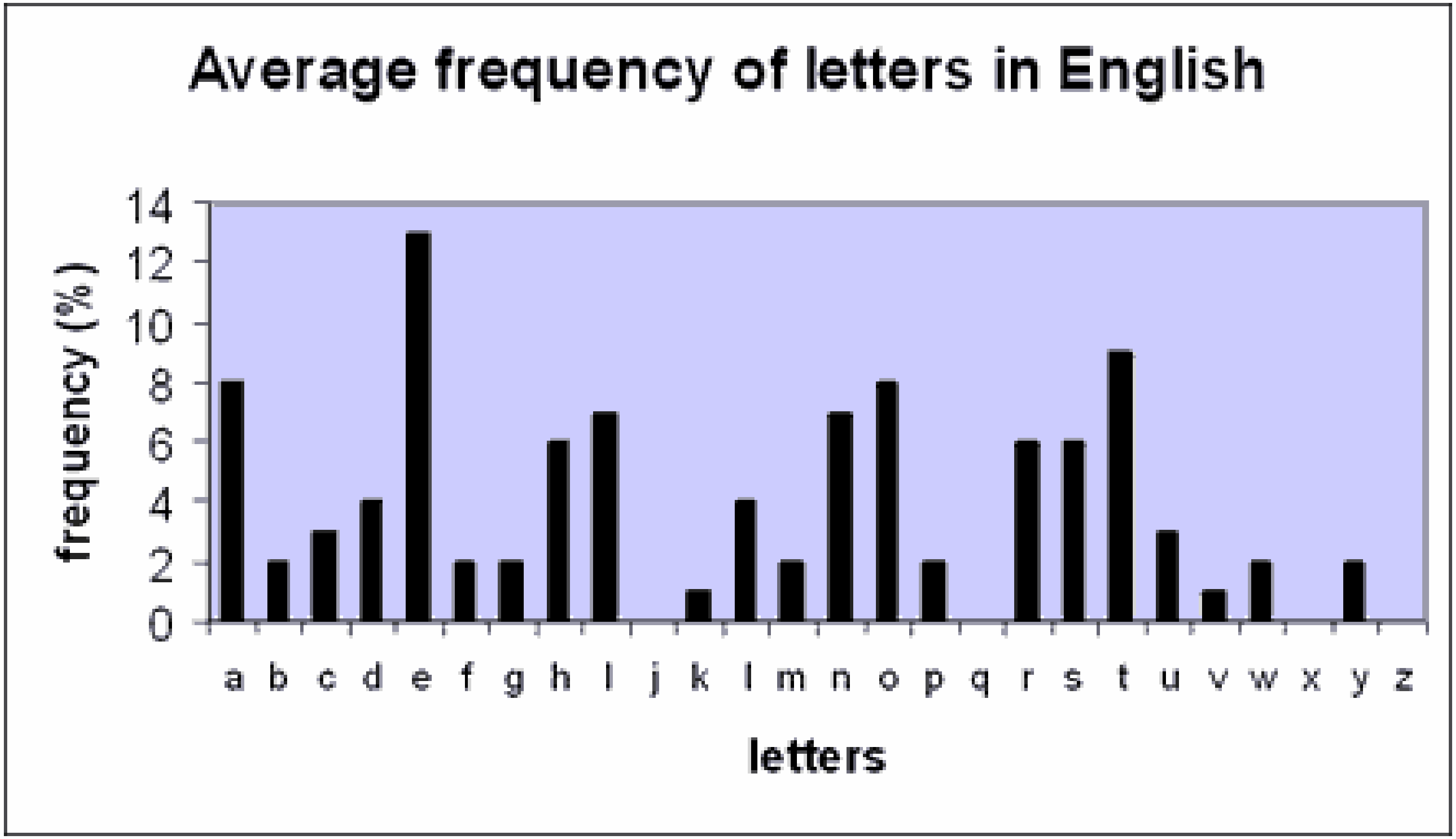
FNNC ZESDQMNNM !

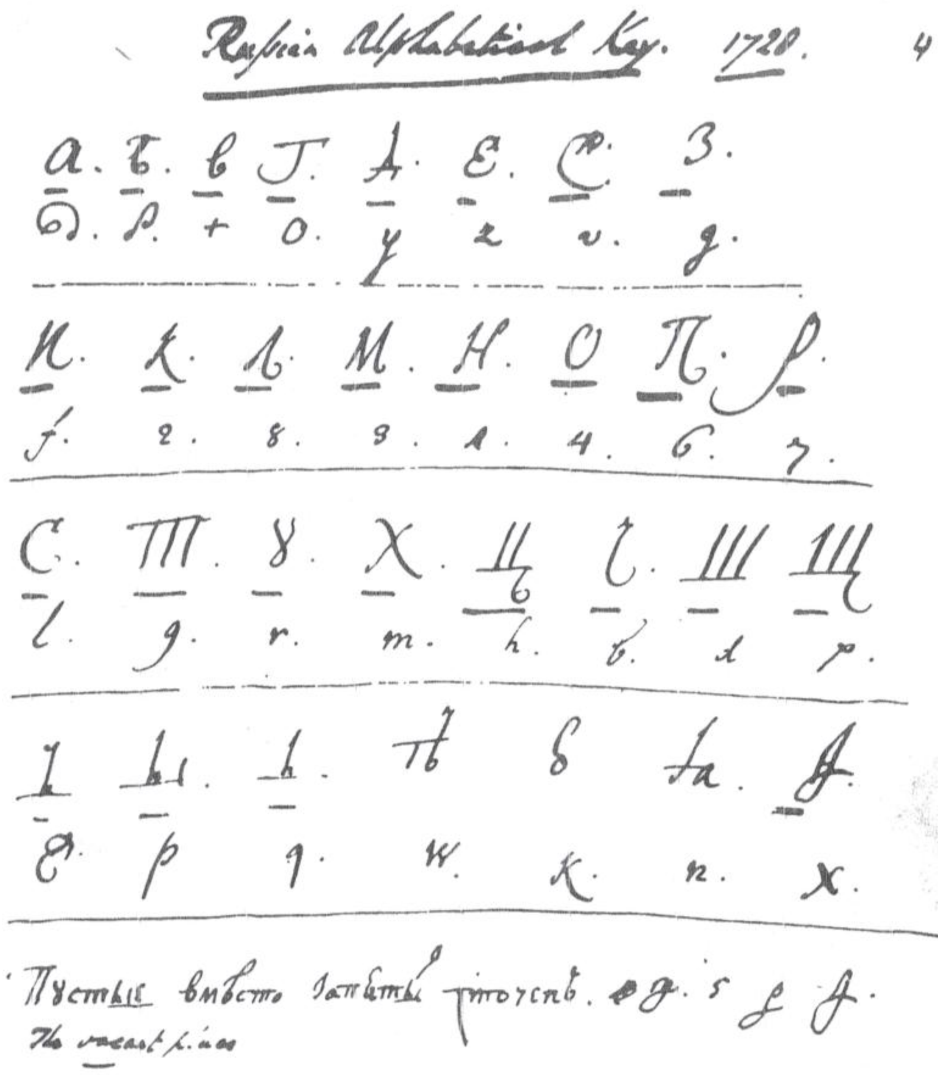
Sghr kdbstqd hr zants dmbqxoshnm

Solving simple substitution ciphers

- Frequency analysis has been known since the 9th century.
- Al Kindi’s *Manuscript on Deciphering Cryptographic Messages*

Yaqub Ibn Ishaq al-Kindi (801-873)


Average frequency of letters in English
frequency (%)
0
2
4
6
8
10
12
14
a b c d e f g h i j k l m n o p q r s t u v w x y z
letters



Russian Alphabetical key. 1728. 4

а.	б.	в	г.	д.	е.	ж.	з.
ϭ.	ρ.	+	o.	y	z	v.	g.
и.	к.	л.	м.	н.	о	п.	р.
f.	2.	8.	3.	1.	4.	6.	7.
с.	т.	у.	х.	ц.	ч.	ш	щ
l.	g.	r.	m.	h.	b.	d	p.
ъ	ы.	ь.	ѣ	ȣ	ꙗ.	ѳ.	
e.	p	q.	w.	k.	n.	x.	

Пустыѣ вмѣсто запятыѣ и точекъ. eg. 5 ʃ ϑ.
The vacant places

Russian monalphabetic key, recovered by England's Decyphering Branch, 1728

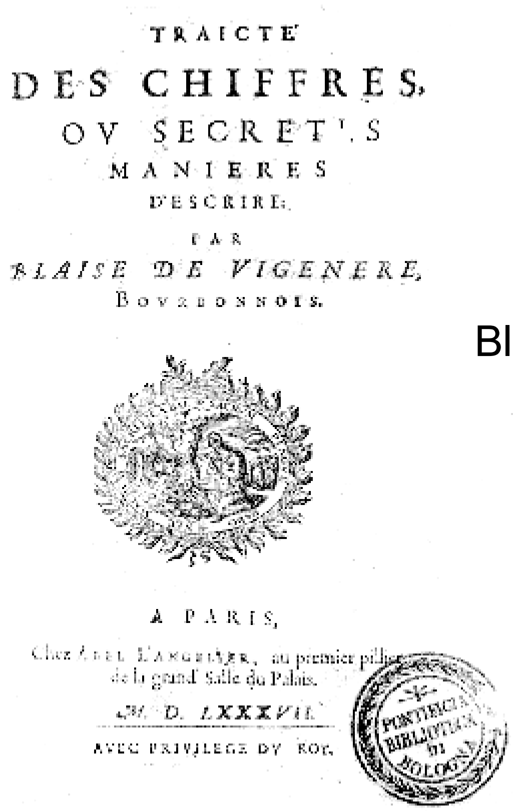
- Russian monoalphabetic substitution key, recovered by England's Decyphering Branch, 1728

- From David Kahn, *The Codebreakers*

2nd Maxim of the Day

- Throughout history, people continued to use insecure encryption methods –long after these methods have been broken – because of ignorance, laziness or force of habit.
- Today also, people use insecure encryption (or no encryption at all). Many technology companies market encryption products that use methods that are insecure, or outright bogus.

Vigenère Encryption


TRAICTE
DES CHIFFRES,
OV SECRETES
MANIERES
D'ESCRIRE:
PAR
BLAISE DE VIGENERE,
BOVRBONNOIS.

A PARIS,
Chez Abel L'Angelier, au premier pillier
de la grand' Salle du Palais.
M. D. LXXXVII.
AVEC PRIVILEGE DV ROY.

PONTIFICIA BIBLIOTHECA DI BOLOGNA

Blaise de Vigenere (1523-1596)

Leon Battista Alberti (1404-1472)

- Use several Cesar substitutions and cycle through them
- Sequence of substitutions determined by a secret key

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fight fiercely, Harvard! Fight! Fight! Fight!

XWTNU NZ H JQRR ZPRU NOEJ GQXK LTVM IBWL YVG

Breaking Vigenère – (1)

- If the key has length K, then the ciphertext letters K positions apart are specified by the same character in the key …
- And thus is the result of a simple substitution
- And thus can be attacked by frequency analysis

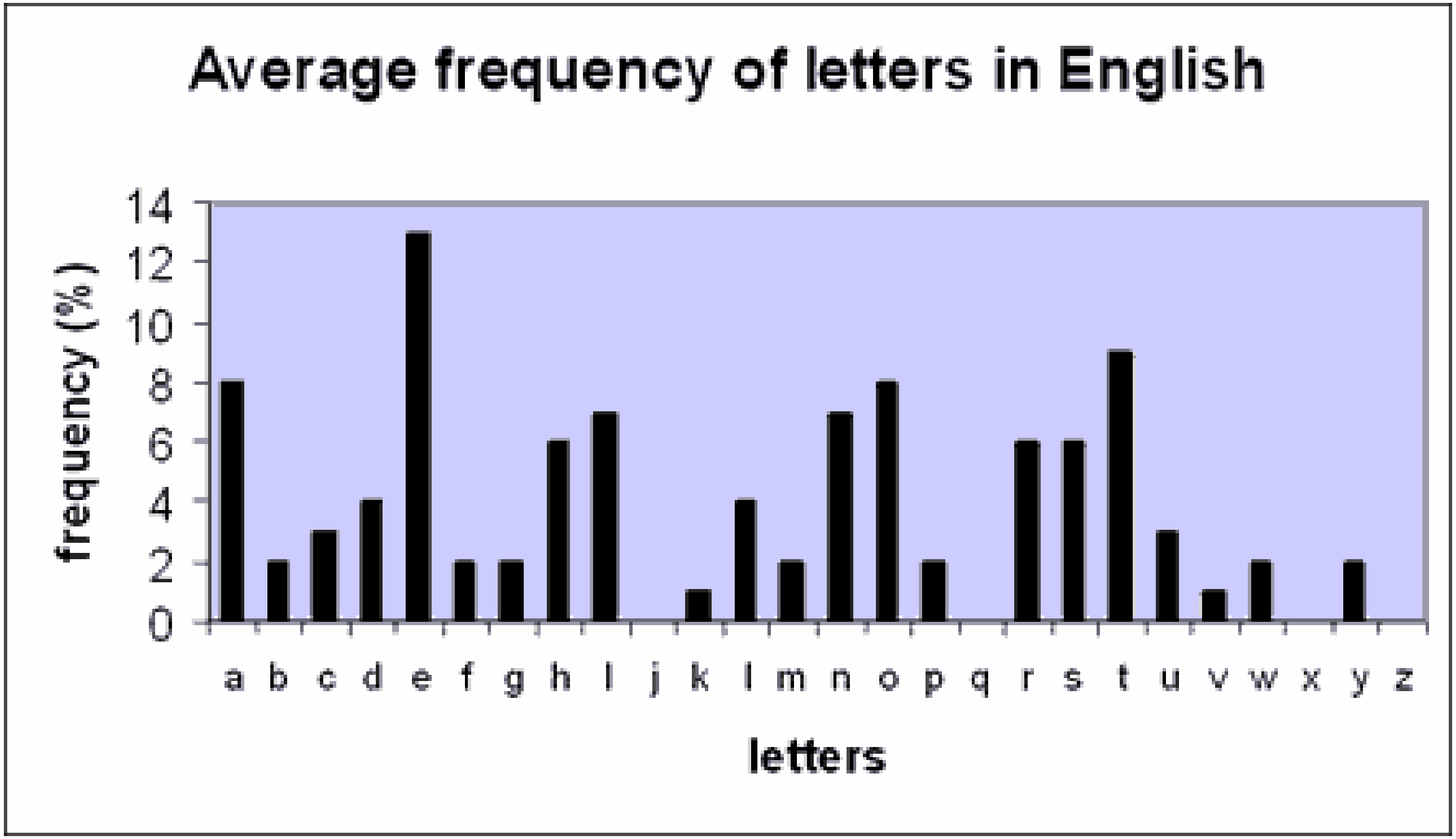
- Example: Suppose the key length is three:

```
DJBK FJWO VJSW FKDS GFJD RKEM CNEJ JKSJ FKDJ SJSS
●●●● ●●●● ●●●● ●●●● ●●●● ●●●● ●●●● ●●●● ●●●● ●●●●
```

So the decryption reduces to doing frequency analysis K times – **provided we know K**

Breaking Vigenère – (2)

- To find the length of the key:
- Try different values for K, looking at every Kth letter of the ciphertext, and pick the one for which the frequency distribution looks like the frequency distribution for English.
- Clever methods to do this by hand:
  - Babbage, Kasiski: counting double letters (1850s, 1860s)
  - Friedman: Index of Coincidence (1920s)
- With computers, we don't need to be clever: Can do brute-force statistics

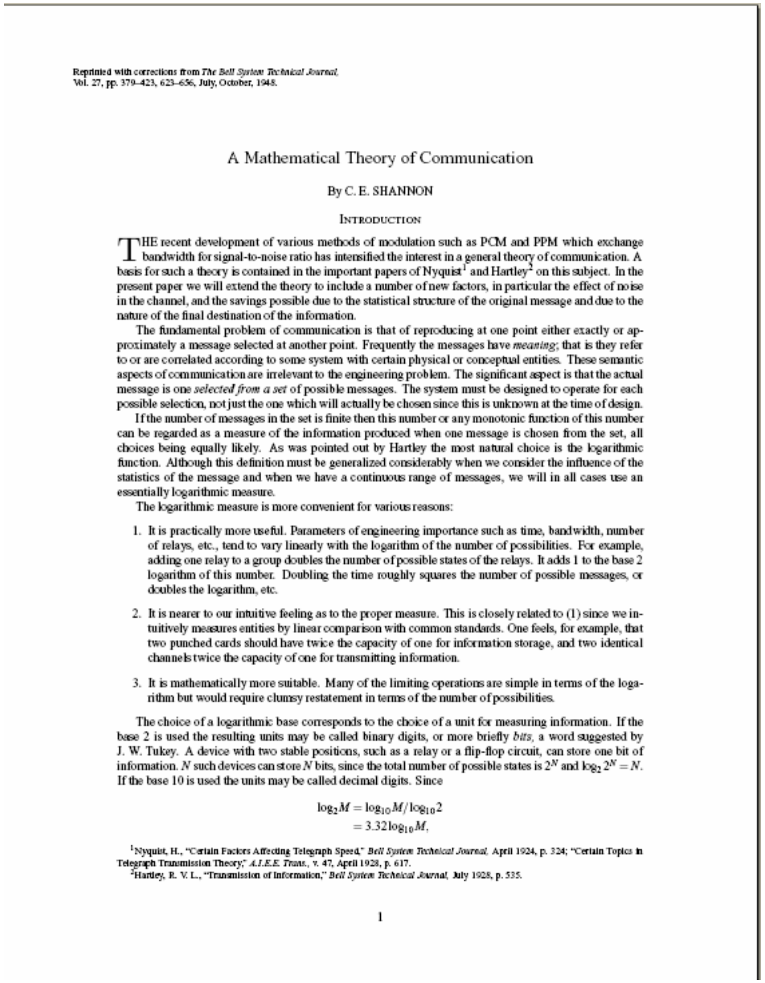

Average frequency of letters in English
frequency (%)
0
2
4
6
8
10
12
14
a b c d e f g h i j k l m n o p q r s t u v w x y z
letters

But suppose the key is as long as the message?

- Then the decryption method breaks down
- A key that is as long as the message is called a **one-time pad.**
- One-time pad encryption is completely secure, provided that
  - the pad is random
  - the pad is used ***only once***

Claude Shannon (1916-2001)

A Mathematical Theory of Communication (1948)



Reprinted with corrections from *The Bell System Technical Journal,*
Vol. 27, pp. 379–423, 623–656, July, October, 1948.

A Mathematical Theory of Communication

By C. E. SHANNON

Introduction

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one *selected from a set* of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design.

If the number of messages in the set is finite then this number or any monotonic function of this number can be regarded as a measure of the information produced when one message is chosen from the set, all choices being equally likely. As was pointed out by Hartley the most natural choice is the logarithmic function. Although this definition must be generalized considerably when we consider the influence of the statistics of the message and when we have a continuous range of messages, we will in all cases use an essentially logarithmic measure.

The logarithmic measure is more convenient for various reasons:

1. It is practically more useful. Parameters of engineering importance such as time, bandwidth, number of relays, etc., tend to vary linearly with the logarithm of the number of possibilities. For example, adding one relay to a group doubles the number of possible states of the relays. It adds 1 to the base 2 logarithm of this number. Doubling the time roughly squares the number of possible messages, or doubles the logarithm, etc.

2. It is nearer to our intuitive feeling as to the proper measure. This is closely related to (1) since we intuitively measures entities by linear comparison with common standards. One feels, for example, that two punched cards should have twice the capacity of one for information storage, and two identical channels twice the capacity of one for transmitting information.

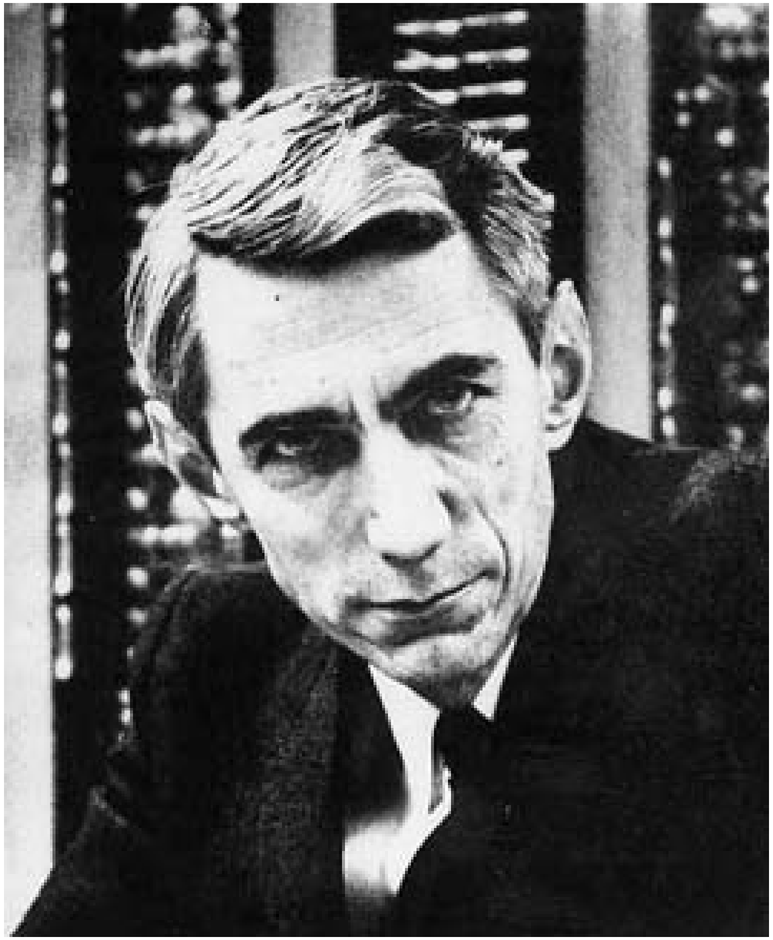
3. It is mathematically more suitable. Many of the limiting operations are simple in terms of the logarithm but would require clumsy restatement in terms of the number of possibilities.

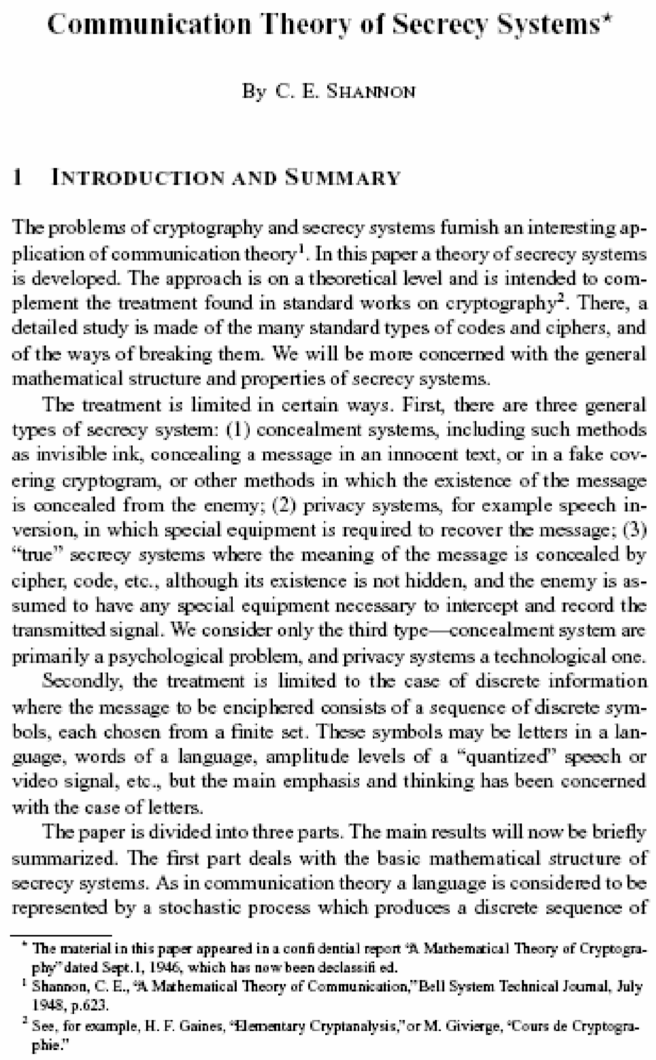
The choice of a logarithmic base corresponds to the choice of a unit for measuring information. If the base 2 is used the resulting units may be called binary digits, or more briefly *bits,* a word suggested by J. W. Tukey. A device with two stable positions, such as a relay or a flip-flop circuit, can store one bit of information. N such devices can store N bits, since the total number of possible states is 2^N and $\log_2 2^N = N$. If the base 10 is used the units may be called decimal digits. Since

$$\begin{aligned} \log_2 M &= \log_{10} M / \log_{10} 2 \\ &= 3.32 \log_{10} M, \end{aligned}$$

[1] Nyquist, H., "Certain Factors Affecting Telegraph Speed," *Bell System Technical Journal,* April 1924, p. 324; "Certain Topics in Telegraph Transmission Theory," *A.I.E.E. Trans.,* v. 47, April 1928, p. 617.

[2] Hartley, R. V. L., "Transmission of Information," *Bell System Technical Journal,* July 1928, p. 535.





Communication Theory of Secrecy Systems*

By C. E. Shannon

1 Introduction and Summary

The problems of cryptography and secrecy systems furnish an interesting application of communication theory[1]. In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography[2]. There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general types of secrecy system: (1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy; (2) privacy systems, for example speech inversion, in which special equipment is required to recover the message; (3) "true" secrecy systems where the meaning of the message is concealed by cipher, code, etc., although its existence is not hidden, and the enemy is assumed to have any special equipment necessary to intercept and record the transmitted signal. We consider only the third type—concealment system are primarily a psychological problem, and privacy systems a technological one.

Secondly, the treatment is limited to the case of discrete information where the message to be enciphered consists of a sequence of discrete symbols, each chosen from a finite set. These symbols may be letters in a language, words of a language, amplitude levels of a "quantized" speech or video signal, etc., but the main emphasis and thinking has been concerned with the case of letters.

The paper is divided into three parts. The main results will now be briefly summarized. The first part deals with the basic mathematical structure of secrecy systems. As in communication theory a language is considered to be represented by a stochastic process which produces a discrete sequence of

[*] The material in this paper appeared in a confidential report "A Mathematical Theory of Cryptography" dated Sept.1, 1946, which has now been declassified.

[1] Shannon, C. E., "A Mathematical Theory of Communication," Bell System Technical Journal, July 1948, p.623.

[2] See, for example, H. F. Gaines, "Elementary Cryptanalysis," or M. Givierge, "Cours de Cryptographie."

- Shannon: “Communication Theory of Secrecy Systems”, 1949
- Based on classified work done in 1946

“Perfect Secrecy” (Shannon, 1949)

- Definition: An encryption system has *perfect secrecy* if knowing the ciphertext tells you no information at all about the plaintext
- Result 1: In order to have perfect secrecy, the key must be as long as the message
- Result 2: A one-time pad system can have perfect secrecy if the pad is truly random

Encrypting with computers

- Want to encrypt *bits* (text, music, images, …), not just letters.
- Rather than shifting letters around, use bit operations like XOR …

Exclusive OR (XOR), a⊕b

- Definition: for two bits, a and b
  - a⊕b = 0 if a and b are the same (both 0 or both 1)
  - a⊕b = 1 if a and b are different
- Combine data bitwise, using XOR
- Example:

  01000010 ⊕ 01010011 = 00010001

XOR encryption (Bit analog of Vigènere)

```
key                SECRET
message            Bill Gates's SSN is  539-60-5125
Repeat key         SECRETSECRETSECRETSECRETSECRETSE
```

message in ASCII

```
   B        i        l        l                5
01000010 01101001 01101100 01101100 ..... 00110101
```

Repeated key in ASCII

```
   S        E        C        R               E
01010011 01000101 01000011 01010010 ..... 01000101
```

Bit-wise xor

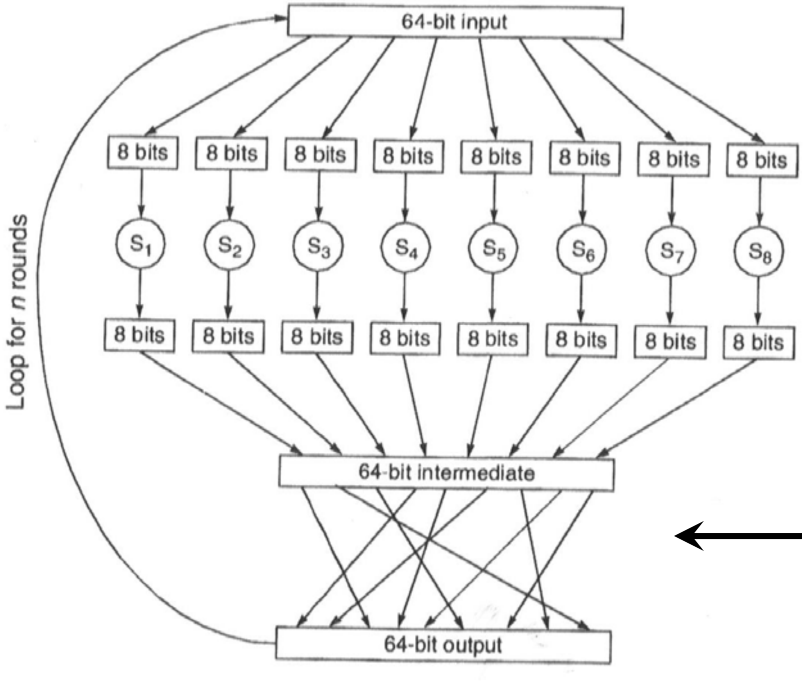
```
00010001 00101100 00101111 00111110 ..... 01110000
```

Encryption methods today

- Insecure methods
  - Lots of them around
    - From hobbyists
    - “Security” startup companies
    - Established companies, as well
- Secure methods
  - One-time pad is the only provably secure method
    - But this requires securely transmitting the pad
  - Many other algorithms that have withstood years of analysis and attempted attacks.

Data Encryption Standard (DES)

- Designed by IBM in 1975, with help from NSA
  - Encrypts 64-bit blocks, based on a 56-bit key



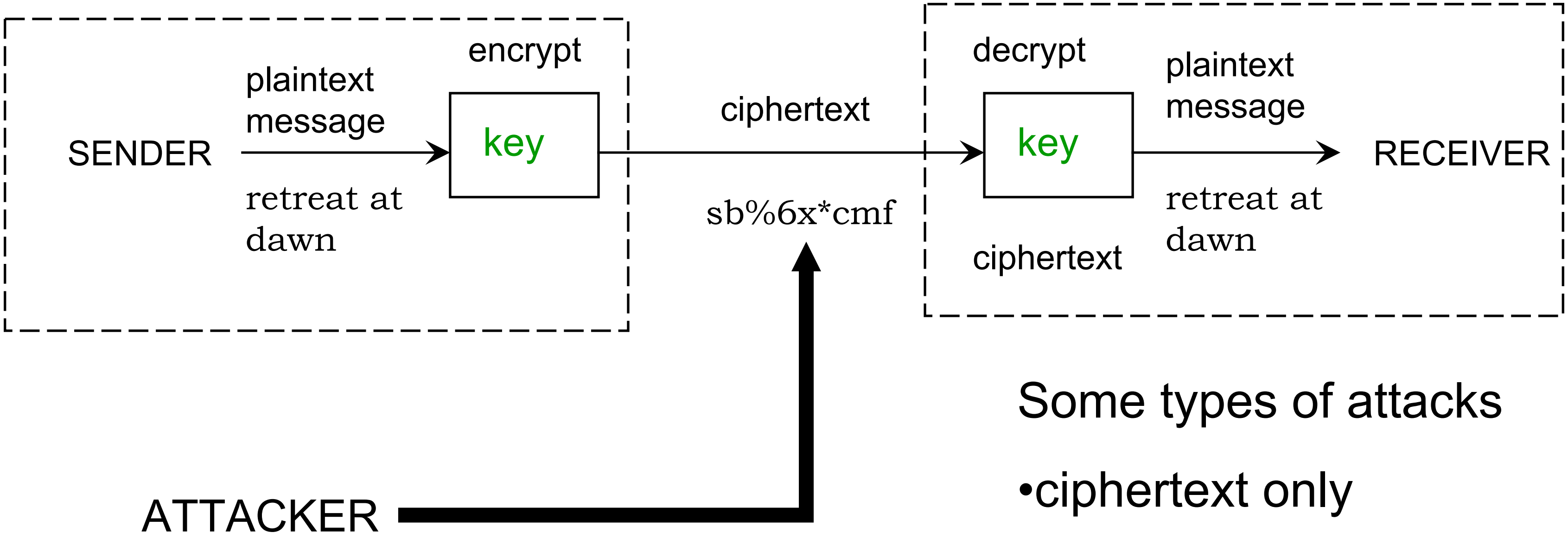
Substitute bit patterns for other bit patterns, based on the key

Shuffle the bits

Security of DES

- No shortcuts, as far as anyone knows
  - You essentially have to try all possible keys
  - Keys are 56 bits long, so there are 2^{56} keys
  - 2^{56} is a big number, but not that big. In August 1998, the Electronic Frontier Foundation demonstrated that a special-purpose machine built from standard parts at a cost of $200,000 could break DES in 56 hours.
- Big governments have a lot more than $200,000 to spend on cryptanalysis.
- Each time you add a bit to the key length, you double the time required to break the system.
- NIST adopted a new Advanced Encryption Standard in 2001 (the Rijndael algorithm, 128-bit keys). DES is still widely used.

Cryptosystems



Some types of attacks

- ciphertext only
- known plaintext
- chosen plaintext
- chosen ciphertext
- rubber hose

Kerkhoffs's Principle

- Auguste Kerkhoffs, *La Cryptographie Militaire*, 1883

- Cryptographic systems should be designed in such a way that they are not compromised if the opponent learns the technique being used. In other words, the security should reside in the choice of key rather than in obscure design features.

  - from Ross Anderson "How to Cheat at the Lottery" (1999)

Schneier quote

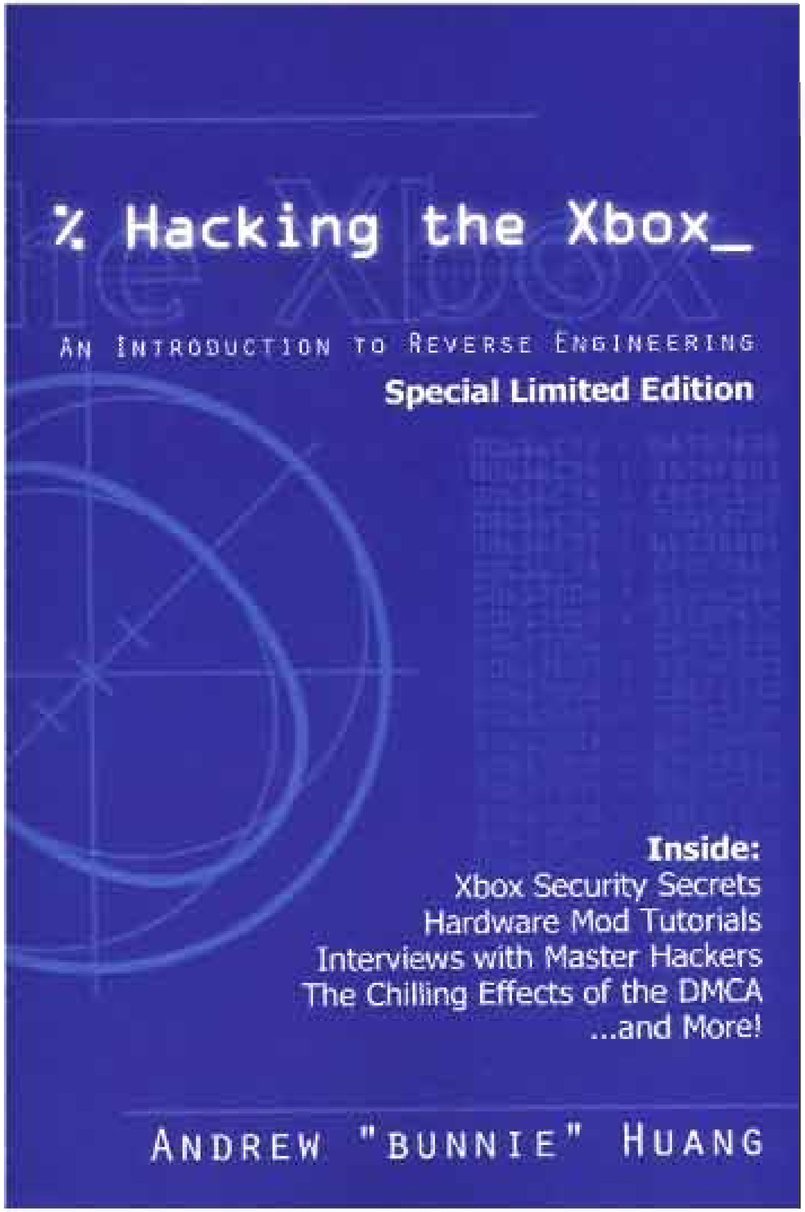
- If the strength of your new cryptosystem relies on the fact that the attacker does not know the algorithm's inner workings, you're sunk. If you believe that keeping the algorithm's insides secret improves the security of your cryptosystem more than letting the academic community analyze it, you're wrong. And if you think that someone won't disassemble your code and reverse-engineer your algorithm, you're naive.
- Bruce Schneier; Applied Cryptography (Second Edition, 1996)

massachusetts institute of technology — artificial intelligence laboratory

Keeping Secrets in Hardware: the Microsoft XBox^{TM} Case Study

Andrew "bunnie" Huang

AI Memo 2002-008   May 26, 2002



% Hacking the Xbox_

An Introduction to Reverse Engineering

Special Limited Edition

Inside:
Xbox Security Secrets
Hardware Mod Tutorials
Interviews with Master Hackers
The Chilling Effects of the DMCA
...and More!

Andrew "bunnie" Huang

None of this is adequate for Internet applications

- In order to communicate, Alice and Bob must share a secret key
  - Doesn’t work well on a large scale
  - Doesn’t work with parties who haven’t made a secure prior arrangement
- But there is a great idea:
- Alice and Bob can create a shared secret key, even if they have never met before and have made no prior arrangements, and even if everyone can eavesdrop on ***all*** their communications …
- … including eavesdropping on the communications they use to establish the key!

End of Part 1

to be continued …

None of this is adequate for Internet applications

- In order to communicate, Alice and Bob must share a secret key
  - Doesn’t work well on a large scale
  - Doesn’t work with parties who haven’t made a secure prior arrangement
- But there is a great idea:
- Alice and Bob can create a shared secret key, even if they have never met before and have made no prior arrangements, and even if everyone can eavesdrop on ***all*** their communications …
- … including eavesdropping on the communications they use to establish the key!

Public-Key Cryptography

Photos removed due to copyright reasons.

The basic idea of Diffie-Hellman-Merkle key agreement

- Arrange things so that
  - Alice computes a number based on secret information that **only Alice knows**
  - Bob computes a number based on secret information that **only Bob knows**
  - Alice and Bob will somehow manage to compute **the same number**, even though they don’t know each other’s secret information
  - No one else can compute this number without knowing Alice’s secret information or Bob’s secret information
- Sounds impossible …

Math Quiz

$$2 \times 6 = 1 \mod 11$$

$$2 \times 6 \times 5 = 5 \mod 11$$

$$2^3 = 1 \mod 7$$

$$2^{300} = 1 \mod 7$$

There's a shortcut for computing powers

- Problem: Given *a* and *p* and *x*, find *y* such that

$$a^x = y \pmod{p}$$

- Method 1: multiply *a* by itself *x* times
  - Requires *x* multiplications
- Method 2: use successive squaring
  - Requires about lg *x* multiplications
- Same idea works for multiplication modulo *p*
- Example: If *x* is a 500-digit number, we can compute $a^x \pmod{p}$ in about 1700 (= lg 10^{500}) steps.

There's no shortcut for computing logarithms mod *p*

- Problem: Given *a* and *p* and *y*, find *x* such that

$$a^x = y \pmod{p}$$

- As far as anyone knows, there are no shortcuts.
  - The only way to do this is essentially by brute-force search among all possibilities for *x*.
- Example: If *p* is a 500-digit number, finding *x* so that

$$a^x = y \pmod{p}$$

requires about 10^{500} steps.

The math behind DHM key agreement

- Given *a* and *p*, and an equation of the form

$$a^x = y \pmod{p}$$

- Then it is exponentially harder to compute *x* given *y*, than it is to compute *y* given *x.*
- For 500-digit numbers, we’re talking about a computing effort of 1700 steps vs. 10^{500} steps.

Diffie-Hellman-Merkle Key Agreement

Start with public, standard values of *p* and *a*

Alice

Pick a secret number S_A

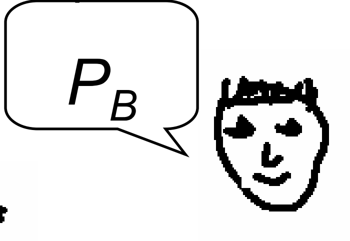
Compute $P_A = a^{S_A} \bmod p$

Shout out P_A

Compute $P_B{}^{S_A} \bmod p$

Eve

Bob



Pick a secret number S_B

Compute $P_B = a^{S_B} \bmod p$

Shout out P_B

Compute $P_A{}^{S_B} \bmod p$

Main point: Alice and Bob have computed the same number, because

$$\left(P_B{}^{S_A} = (a^{S_B})^{S_A} = a^{S_B S_A} = (a^{S_A})^{S_B} = P_A{}^{S_B}\right) \bmod p$$

Alice and Bob can now use this number as a shared key for encrypted communication

Eavesdroppers know $P_A = a^{S_A} \bmod p$ and $P_B = a^{S_B} \bmod p$

But going from these to $a^{S_A S_B} \bmod p$ requires computing logarithms mod *p*, as far as anyone knows

Confidential Email with “Offline Diffie-Hellman-Merkle”

Alice

Alice picks a *secret key* S_A, computes the corresponding *public key* P_A (using the D-H formula) and publishes P_A in a directory

To send Alice a message,

Bob

Looks up Alice’s public key, picks a random number to play the role of $S_{B,}$ for this message, and computes the corresponding P_B (using the D-H formula)

Uses S_B and Alice’s public key to create an encryption key for this message (using the D-H formula)

Sends the encrypted message to Alice, along with P_B

Alice

Uses her secret key and the P_B she received from Bob to compute the key and decrypt the message

But there’s a problem…

- How can Bob know that the listing in the directory is really Alice’s secret key?

Alice

Alice picks a *secret key* S_A, computes the corresponding *public key* P_A and publishes P_A in a directory

Tampers with the directory and inserts her own key under Alice’s name

Eve

Bob

Obliviously uses “Alice’s” public key from the directory, but is in reality sending messages that Eve can decrypt.

Digital signature algorithms

- Given a secret key, the corresponding public key, and a message, generate a number SIG such that
  - SIG is easy to compute if you know the secret key and the message
  - SIG is infeasible to compute if you don't know the secret key
  - SIG is easy to "check" by anyone who knows the message and the public key. That is, a certain condition involving the message and SIG and the public key must be valid
- Digital signature algorithms are a lot like the Diffie-Hellman-Merkle algorithm
- RSA (Rivest-Shamir-Adleman) was the first practical system to do digital signatures, and it *also* did public-key encryption

Using digital signatures

- To sign a message, you computes SIG using your secret key. Anyone can check SIG using your public key.
- If the message was tampered with, the signature won’t check. [integrity]
- No one other than you could have produced SIG, since producing SIG requires knowing your secret key. [authentication and non-repudiation]

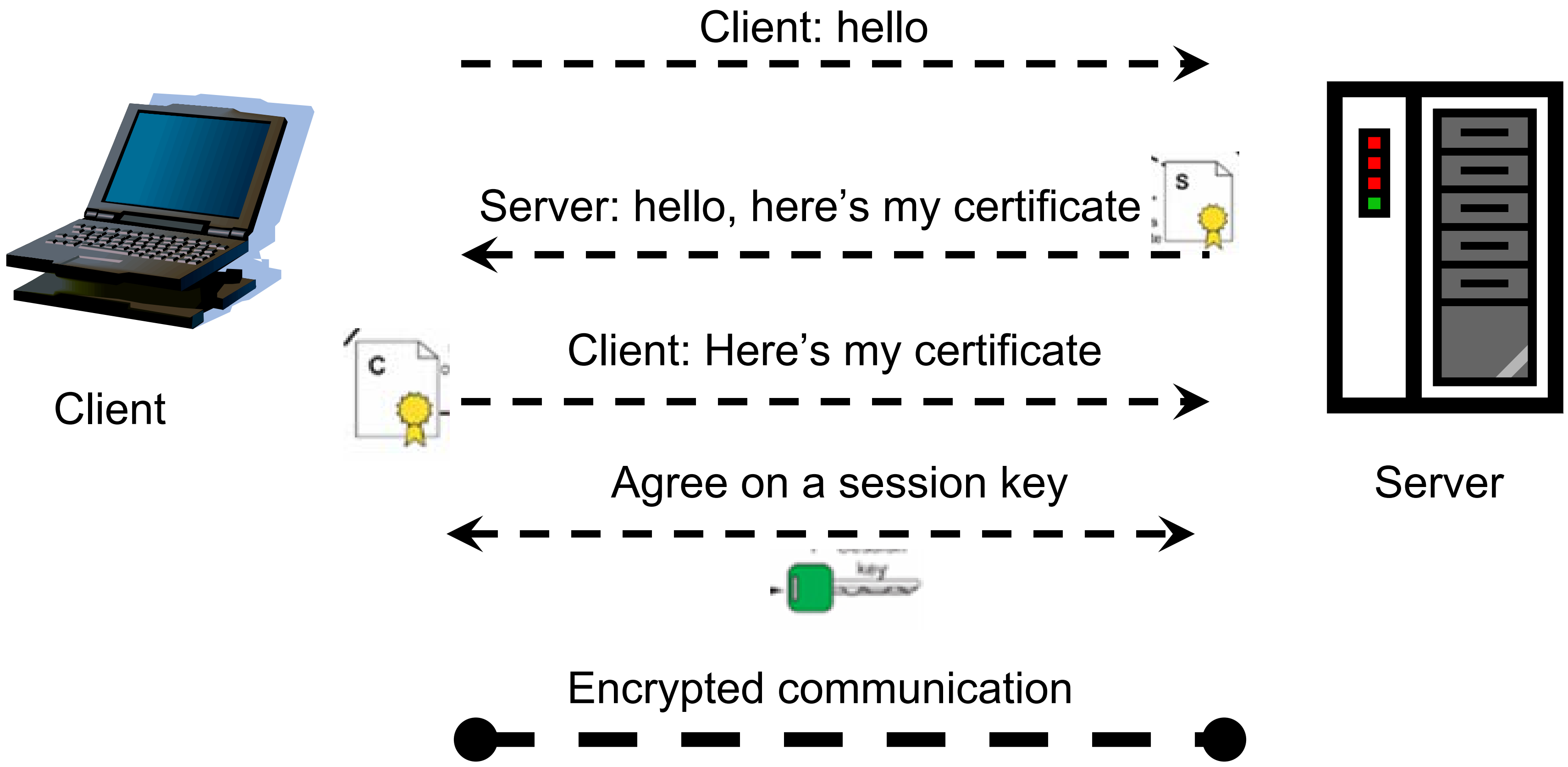
Certificates and Certifying Authorities*

Public Key Infrastructures (PKI)

- How do we know that "Alice's public key" actually belongs to Alice?
  - Alice goes to a *Certification Authority* (CA), demonstrates her identity, and shows her public key. The CA digitally signs Alice's public key, producing a *certificate.* Anyone can check the validity of the certificate by using the CA's public key.
- How do we know the CA's public key is really the CA's public key?
  - 1. The CA also has a certificate, signed by some well-known and trusted authority like the US Post Office (chain of trust); and/or
  - 2. Lots of people we trust have vouched for it (web of trust)

*Loren M Kohnfelder. *Towards a Practical Public-key Cryptosystem*. Bachelor's thesis, EECS Dept., Massachusetts Institute of Technology, May, 1978.

Basic Transport Layer Security Protocol (old name: SSL)



Client: hello

Server: hello, here’s my certificate

Client: Here’s my certificate

Agree on a session key

Encrypted communication

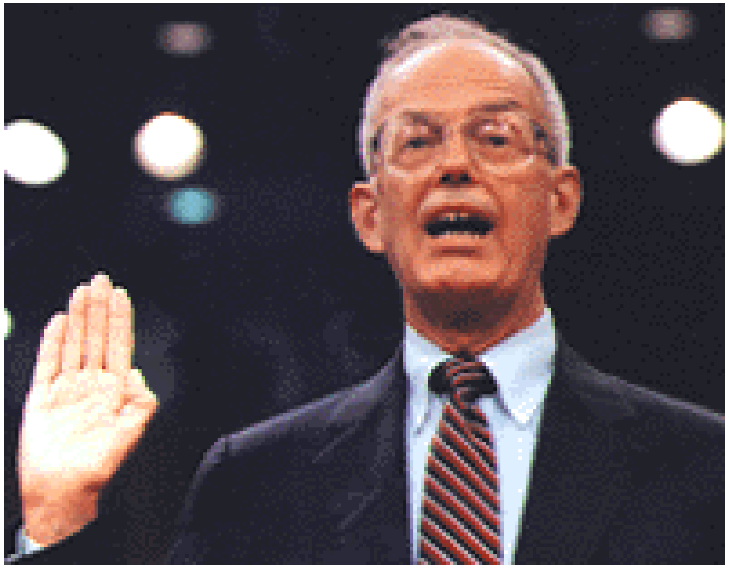
Client

Server

End of Part 2

to be continued …

National Security Agency



There is a very real and critical danger that unrestrained public discussion of cryptologic matters will seriously damage the ability of this government to conduct signals intelligence and the ability of this government to carry out its mission of protecting national security information from hostile exploitation.

-- Admiral Bobby Ray Inman (Director of the NSA, 1979)

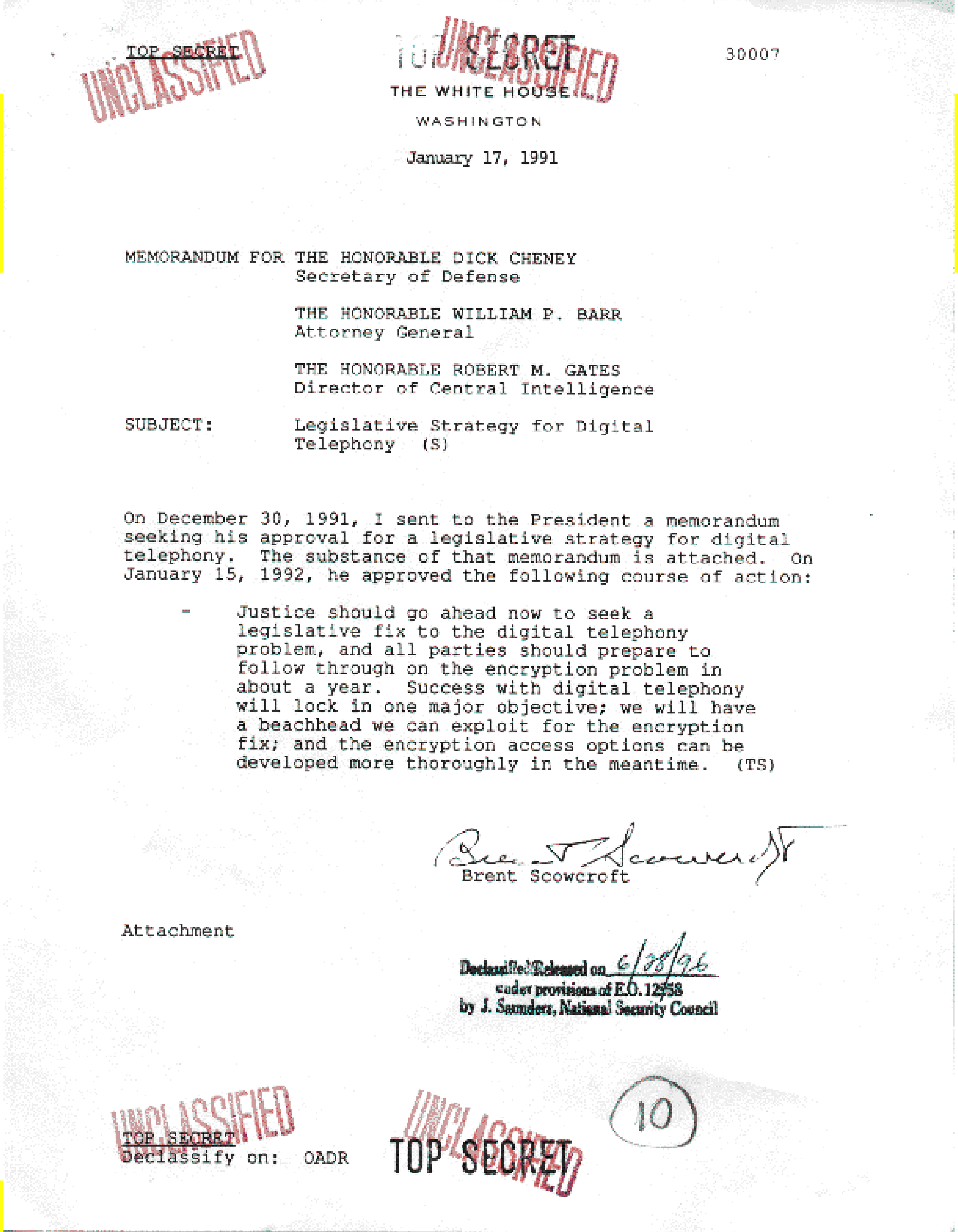
FEDERAL BUREAU OF INVESTIGATION

FBI Director Louis Freeh,
Congressional testimony
March 30, 1995

Unless the issue of encryption is resolved soon, criminal conversations over the telephone and other communications devices will become indecipherable by law enforcement. This, as much as any issue, jeopardizes the public safety and national security of this country. Drug cartels, terrorists, and kidnappers will use telephones and other communications media with impunity knowing that their conversations are immune from our most valued investigative technique.

CALEA, October 1994

… a telecommunications carrier … shall ensure that its equipment, facilities, or services … are capable of … expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept … all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government …



~~TOP SECRET~~ UNCLASSIFIED

~~TOP SECRET~~ UNCLASSIFIED

30007

THE WHITE HOUSE

WASHINGTON

January 17, 1991

MEMORANDUM FOR THE HONORABLE DICK CHENEY
Secretary of Defense

THE HONORABLE WILLIAM P. BARR
Attorney General

THE HONORABLE ROBERT M. GATES
Director of Central Intelligence

SUBJECT: Legislative Strategy for Digital Telephony (S)

On December 30, 1991, I sent to the President a memorandum seeking his approval for a legislative strategy for digital telephony. The substance of that memorandum is attached. On January 15, 1992, he approved the following course of action:

- Justice should go ahead now to seek a legislative fix to the digital telephony problem, and all parties should prepare to follow through on the encryption problem in about a year. Success with digital telephony will lock in one major objective; we will have a beachhead we can exploit for the encryption fix; and the encryption access options can be developed more thoroughly in the meantime. (TS)

Brent Scowcroft

Attachment

Declassified/Released on 6/28/96
under provisions of E.O. 12958
by J. Saunders, National Security Council

UNCLASSIFIED
~~TOP SECRET~~
Declassify on: OADR

~~TOP SECRET~~ UNCLASSIFIED

10

Telephony (S)

On December 30, 1991, I sent to the President a memorandum seeking his approval for a legislative strategy for digital telephony. The substance of that memorandum is attached. On January 15, 1992, he approved the following course of action:

- Justice should go ahead now to seek a legislative fix to the digital telephony problem, and all parties should prepare to follow through on the encryption problem in about a year. Success with digital telephony will lock in one major objective; we will have a beachhead we can exploit for the encryption fix; and the encryption access options can be developed more thoroughly in the meantime. (TS)

Brent Scowcroft

Attachment

Declassified/Released on 6/28/96
under provisions of E.O. 12958
by J. Saunders, National Security Council

UNCLASSIFIED

TOP SECRET
Declassify on: OADR

TOP SECRET

UNCLASSIFIED

10

Clipper

- Designed by the NSA: “For telephones only”
- Authorized by classified Clinton directive in April 1993 (publicly announced only that they were evaluating it). Standards released in Feb. 1994
- “Voluntary” (but government will buy only Clipper phones)
- Built-in (“back door”) key that is split: each half held by a different government agency (“key escrow”)
- Encryption algorithm classified: Clipper chips must be tamperproof and therefore expensive
- Clipper phones do not interoperate with non-Clipper phones
- “Capstone” chip for computer data and communications

The key escrow wars

- Dramatis Personae
  - Industry
  - Law enforcement
  - National security
  - Civil libertarian groups

Government's big hammer: Crypto export controls

- Pre-1995: Encryption technology classified by State Department as a munition
  - Illegal to export hardware, software, technical information, unless you register as an arms dealer and adhere to stringent regulations
  - Illegal to provide material or technical assistance to non-US personnel, including posting on the internet to be available outside the US
- 1995: *Bernstein v. US Dept. of State, et. al.*, suit filed challenging the Constitutionality of export regulations
- 1996: Jurisdiction for crypto exports transferred to Commerce Department, but restrictions remain.
- 1996-2001: Crypto regulations modified and relaxed, but still exist (e.g., can't export to the CIILNKSS countries)
- 2003: Bernstein case still in the courts

Industry claims and issues (1995)

- Customers want security for electronic commerce, for protecting remote access, for confidentiality of business information.
- Export restrictions are a pain in the butt.
- There is plausible commercial demand for “exceptional access” to stored encrypted data (e.g., is someone loses a key); but little demand for access to encrypted communications, and no commercial demand for surreptitious access.

Law enforcement claims and issues (1995)

- Wiretapping is a critical law-enforcement tool.
- Wiretaps are conducted on specific, identified targets under lawful authority.
- For wiretapping, access to escrowed keys must occur without knowledge of the keyholders.
- Many criminals are often sloppy and/or stupid: They won’t use encryption unless it becomes ubiquitous. Some criminals are far from sloppy or stupid: They will use encryption if it is available.
- Evidence obtained from decryption must hold up in court.
- There is a need for international cooperation in law enforcement.

National security establishment claims and issues (1995)

- We can’t tell you, but they are really serious.
- NSA “is rumored to be” carrying out blanket interceptions of communications on a massive scale, using computers to filter out the interesting traffic.

echelonwatch

EUROPEAN PARLIAMENT

1999 *2004*

Session document

11 July 2001

FINAL REPORT

on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)

Civil libertarian claims and issues (1995)

- As computer communication technology becomes more pervasive, allowing government access to communications becomes much more than traditional wiretapping of phone conversations.
- How do we guard against abuse of the system?
- If we make wiretapping easy, then what are the checks on its increasing use?
- There are other tools (bugging, data mining, DNA matching) that can assist law enforcement. People have less privacy than previously, even without wiretapping.

NIST meetings with industry, Fall 95

- Allow export of hardware and software with up to 56-bit algorithms, provided the keys are escrowed with government approved “escrow agents”
- But
  - no interoperability between escrowed and non-escrowed systems
  - escrow cannot be disabled
  - escrow agents must be certified by US government or by foreign governments with whom US has formal agreements

- Talks broke down

Interagency working group draft, May 96

- *Industry and government must partner in the development of a public key-based key management infrastructure and attendant products that will assure participants can transmit and receive information electronically with confidence in the information's integrity, authenticity, and origin and which will assure timely lawful government access.*
- Escrow is the price of certification (CA might be also function as an EA)

Courting industry, Fall 96 - ...

- Shift jurisdiction of crypto exports from State to Commerce
- Allow export of any strength, so long as it has key escrow (now known as “key recovery” - KR)
- Immediate approval of export for 56-bit DES, provided company files a plan for installing KR in new 56-products within two years
- Increased granting of export licenses for restricted applications (e..g, financial transactions)

Legislation, 1997

- Bills introduced all over the map, ranging from elimination of export controls to bills that would mandate key recovery for domestic use.

THE RISKS OF KEY RECOVERY, KEY ESCROW, & TRUSTED THIRD PARTY ENCRYPTION

A Report by an Ad Hoc Group of Cryptographers and Computer Scientists

- Hal Abelson
- Ross Anderson
- Steven M. Bellovin
- Josh Benaloh
- Matt Blaze
- Whitfield Diffie
- John Gilmore
- Peter G. Neumann
- Ronald L. Rivest
- Jeffrey I. Schiller
- Bruce Schneier

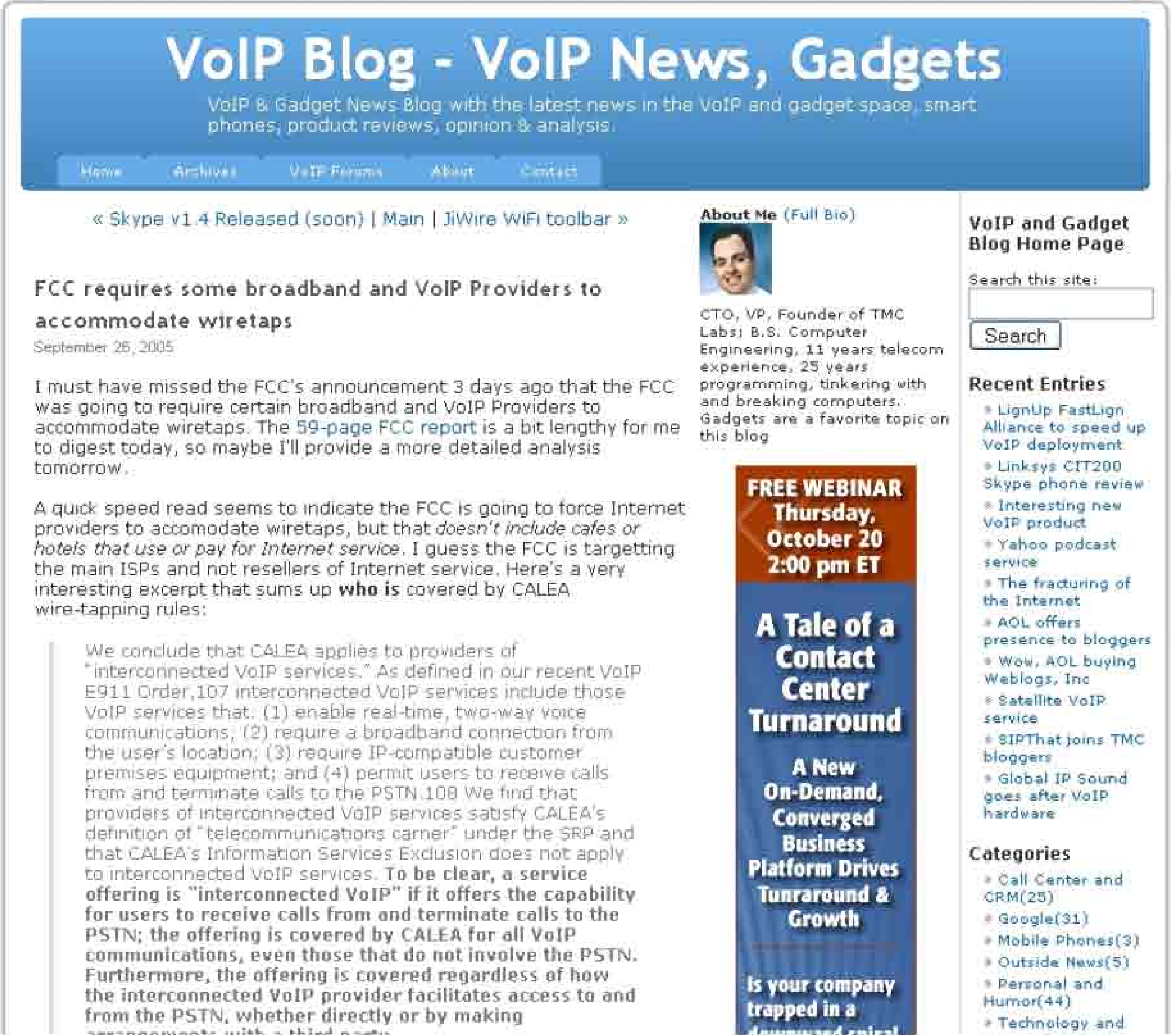
Some technical observations

- If Alice and Bob can authenticate to each other, then they can use Diffie-Hellman to establish a shared key for communications
- The security requirements for CAs are very different from those for escrow agents
- Implementing basic crypto is cheap, adding a key recovery infrastructure is not.
- Crypto is necessary not only for electronic commerce, but to protect the information infrastructure. But key escrow may make things less secure, not more:
  - Repositories of escrowed keys could be irresistible targets of attack by criminals
  - If thousands of law enforcement personnel can quickly get access to escrowed keys, then **who else can??**

More recently …

- Jan, 2000: Commerce Department issues new export regulations on encryption, relaxing restrictions
- Sept. 13, 2001: Sen. Judd Gregg (New Hampshire) calls for encryption regulations, saying encryption makers “have as much at risk as we have at risk as a nation, and they should understand that as a matter of citizenship, they have an obligation” to include decryption methods for government agents.
- By Oct., Gregg had changed his mind about introducing legislation.

Question: Why was 2001 so different from 1997?



VoIP Blog - VoIP News, Gadgets

VoIP & Gadget News Blog with the latest news in the VoIP and gadget space, smart phones, product reviews, opinion & analysis.

« Skype v1.4 Released (soon) | Main | JiWire WiFi toolbar »

FCC requires some broadband and VoIP Providers to accommodate wiretaps

September 26, 2005

I must have missed the FCC's announcement 3 days ago that the FCC was going to require certain broadband and VoIP Providers to accommodate wiretaps. The 59-page FCC report is a bit lengthy for me to digest today, so maybe I'll provide a more detailed analysis tomorrow.

A quick speed read seems to indicate the FCC is going to force Internet providers to accomodate wiretaps, but that *doesn't include cafes or hotels that use or pay for Internet service*. I guess the FCC is targetting the main ISPs and not resellers of Internet service. Here's a very interesting excerpt that sums up **who is** covered by CALEA wire-tapping rules:

> We conclude that CALEA applies to providers of "interconnected VoIP services." As defined in our recent VoIP E911 Order,107 interconnected VoIP services include those VoIP services that: (1) enable real-time, two-way voice communications; (2) require a broadband connection from the user's location; (3) require IP-compatible customer premises equipment; and (4) permit users to receive calls from and terminate calls to the PSTN.108 We find that providers of interconnected VoIP services satisfy CALEA's definition of "telecommunications carrier" under the SRP and that CALEA's Information Services Exclusion does not apply to interconnected VoIP services. **To be clear, a service offering is "interconnected VoIP" if it offers the capability for users to receive calls from and terminate calls to the PSTN; the offering is covered by CALEA for all VoIP communications, even those that do not involve the PSTN. Furthermore, the offering is covered regardless of how the interconnected VoIP provider facilitates access to and from the PSTN, whether directly or by making arrangements with a third party.**

About Me (Full Bio)

CTO, VP, Founder of TMC Labs; B.S. Computer Engineering, 11 years telecom experience, 25 years programming, tinkering with and breaking computers. Gadgets are a favorite topic on this blog

VoIP and Gadget Blog Home Page

Search this site:

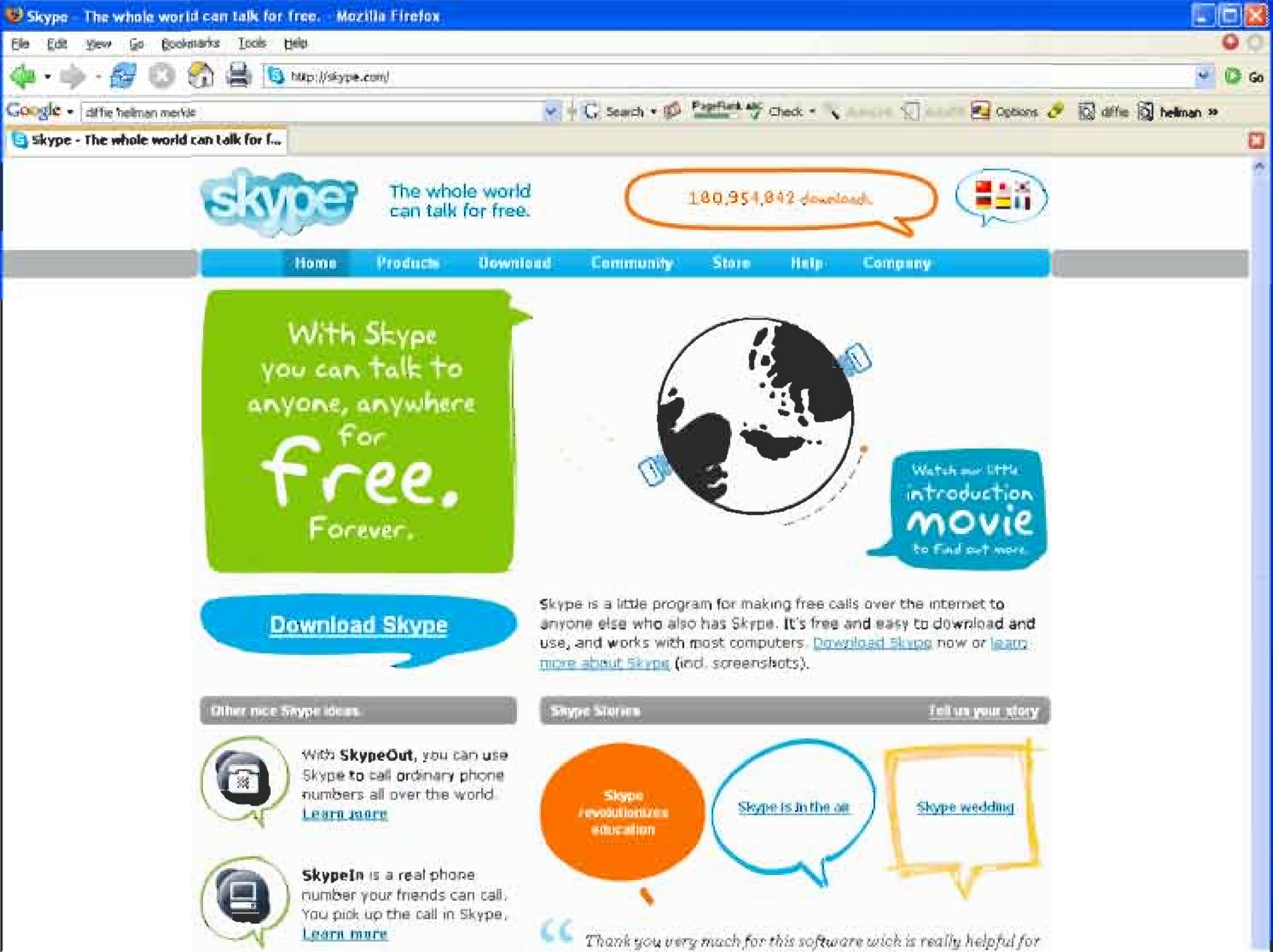
Search

Recent Entries

- LignUp FastLign Alliance to speed up VoIP deployment
- Linksys CIT200 Skype phone review
- Interesting new VoIP product
- Yahoo podcast service
- The fracturing of the Internet
- AOL offers presence to bloggers
- Wow, AOL buying Weblogs, Inc
- Satellite VoIP service
- SIPThat joins TMC bloggers
- Global IP Sound goes after VoIP hardware

Categories

- Call Center and CRM(25)
- Google(31)
- Mobile Phones(3)
- Outside News(5)
- Personal and Humor(44)
- Technology and



Skype - The whole world can talk for free. - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://skype.com/
Go
Google
diffie hellman merkle
Search
PageRank
Check
Options
diffie
hellman
Skype - The whole world can talk for f...
skype
Home
Products
Download
Community
Store
Help
Company

The whole world can talk for free.

180,954,842 downloads

With Skype you can talk to anyone, anywhere for free. Forever.

Watch our little introduction movie to find out more.

Download Skype

Skype is a little program for making free calls over the internet to anyone else who also has Skype. It's free and easy to download and use, and works with most computers. Download Skype now or learn more about Skype (incl. screenshots).

Other nice Skype ideas

With **SkypeOut**, you can use Skype to call ordinary phone numbers all over the world. Learn more

SkypeIn is a real phone number your friends can call. You pick up the call in Skype. Learn more

Skype Stories

Tell us your story

Skype revolutionizes education

Skype is in the air

Skype wedding

“ *Thank you very much for this software wich is really helpful for*

END