Keeping Secrets

What you need to know about Encryption

DeeDee Lavinder

@ddlavinder

One letter stands for another. In this sample, A is used for the three L's, X for the two O's, etc. Single letters, apostrophes, the length and formation of the words are all hints. Each day the code letters are different.

10-9 **CRYPTOQUOTE**

APK GP OPM YRIG CA UBMMBOE SRPSYR PQRT MUR URIG — MUIM'Z IZZIKYM, OPM YRIGRTZUBS. — GHBEUM G. RBZROUPHRT

Cryptography

Encryption

Scytale

Cipher


Zur Beachtung!

[24] ~~CONFIDENTIAL~~ (P7)

E-1791-B (4-44)

COVER SHEET FOR TECHNICAL MEMORANDA
RESEARCH DEPARTMENT

SUBJECT: A Mathematical Theory of Cryptography - Case 20878 (4)

ROUTING:
1 – HWB-HF-Case Files
2 – CASE FILES
3 – J. W. McRae
4 – L. Espenschied
5 – H. S. Black
6 – F. B. Llewellyn
7 – H. Nyquist
8 – B. M. Oliver
9 – R. K. Potter
10 – C. B. H. Feldman
11 - R. C. Mathes
12 - R. V. L. Hartley
13 - J. R. Pierce
14 - H. W. Bode
15 - R. L. Dietzold
16 - L. A. MacCall
17 - W. A. Shewhart
18 - S. A. Schelkunoff
19 - C. E. Shannon
20 - Dept. 1000 Files

MM– 45-110-92
DATE September 1, 1945
AUTHOR C. E. Shannon
INDEX NO. P 0.4

SECRET

~~ABSTRACT~~

DOWNGRADED AT 3 YEAR INTERVALS
DECLASSIFIED AFTER 12 YEARS
DOD DIR 5200.10

ABSTRACT

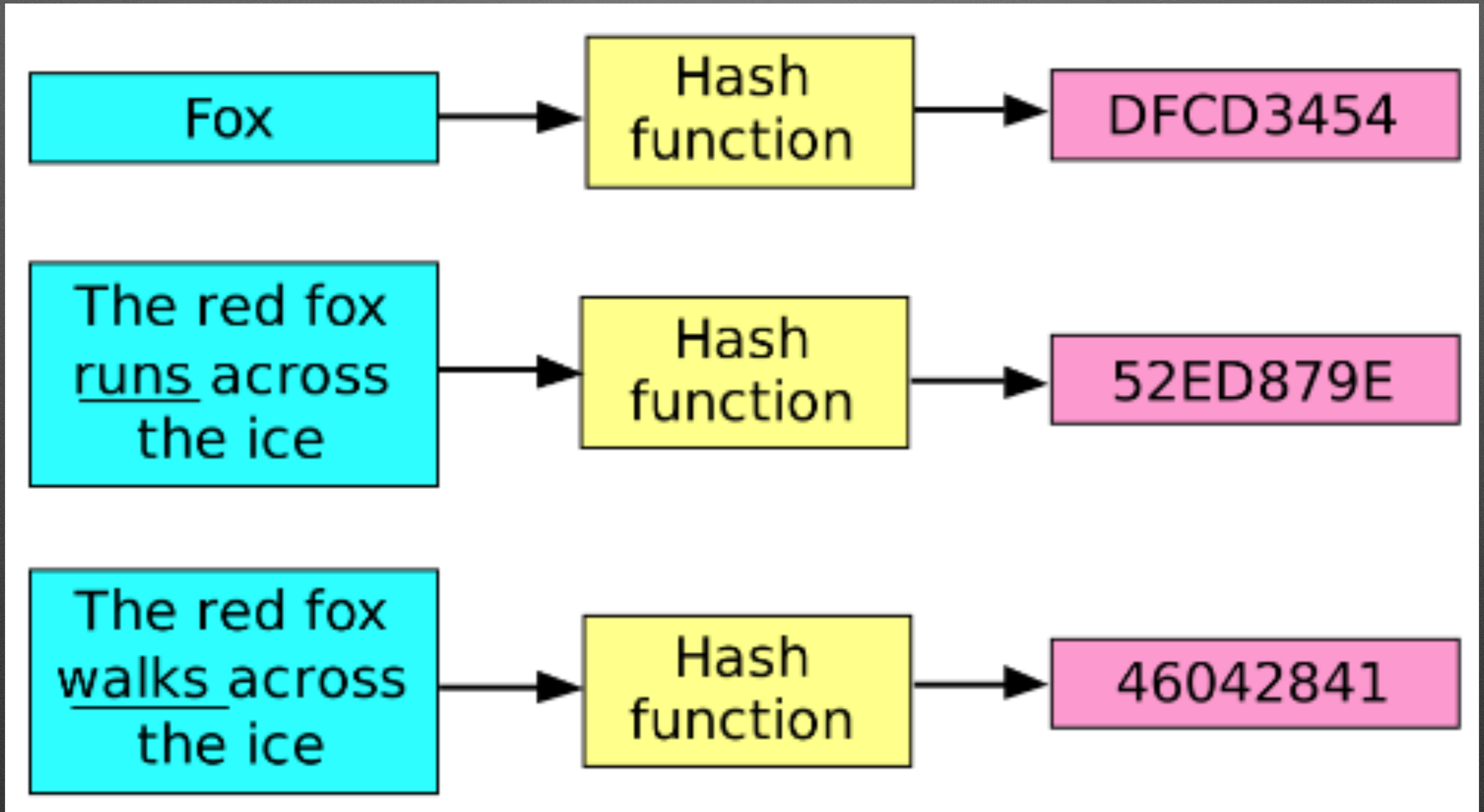
A mathematical theory of secrecy systems is developed. Three main problems are considered. (1) A logical formulation of the problem and a study of the mathematical structure of secrecy systems. (2) The problem of "theoretical secrecy," i.e., can a system be solved given unlimited time and how much material must be intercepted to obtain a unique solution to cryptograms. A secrecy measure called the "equivocation" is defined and its properties developed. (3) The problem of "practical secrecy." How can systems be made difficult to solve, even though a solution is theoretically possible.

THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE LAWS, TITLE 18 U.S.C., SECTIONS 793 AND 794. ITS TRANSMISSION OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW.

~~CONFIDENTIAL~~

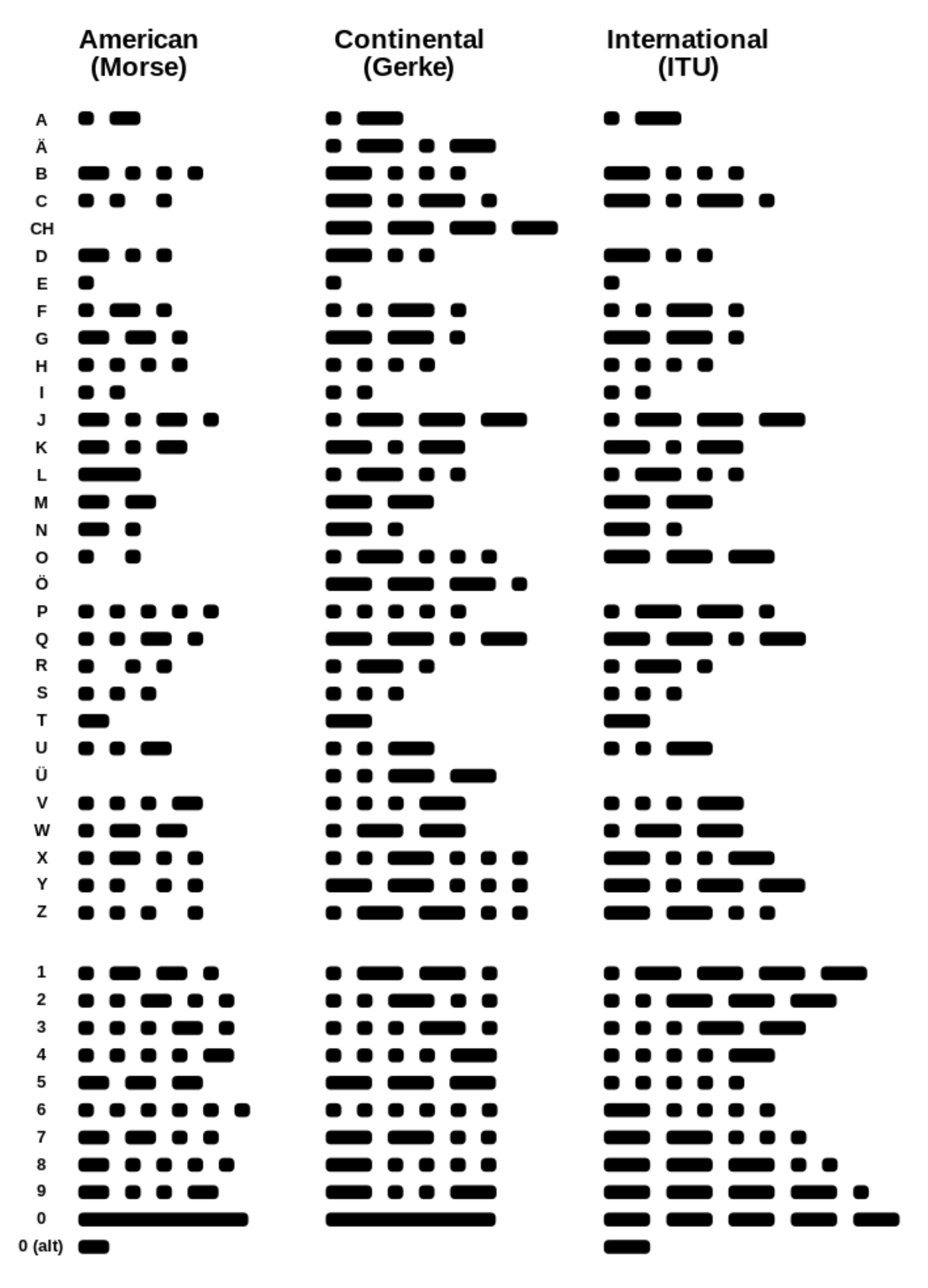
Encryption != Hash

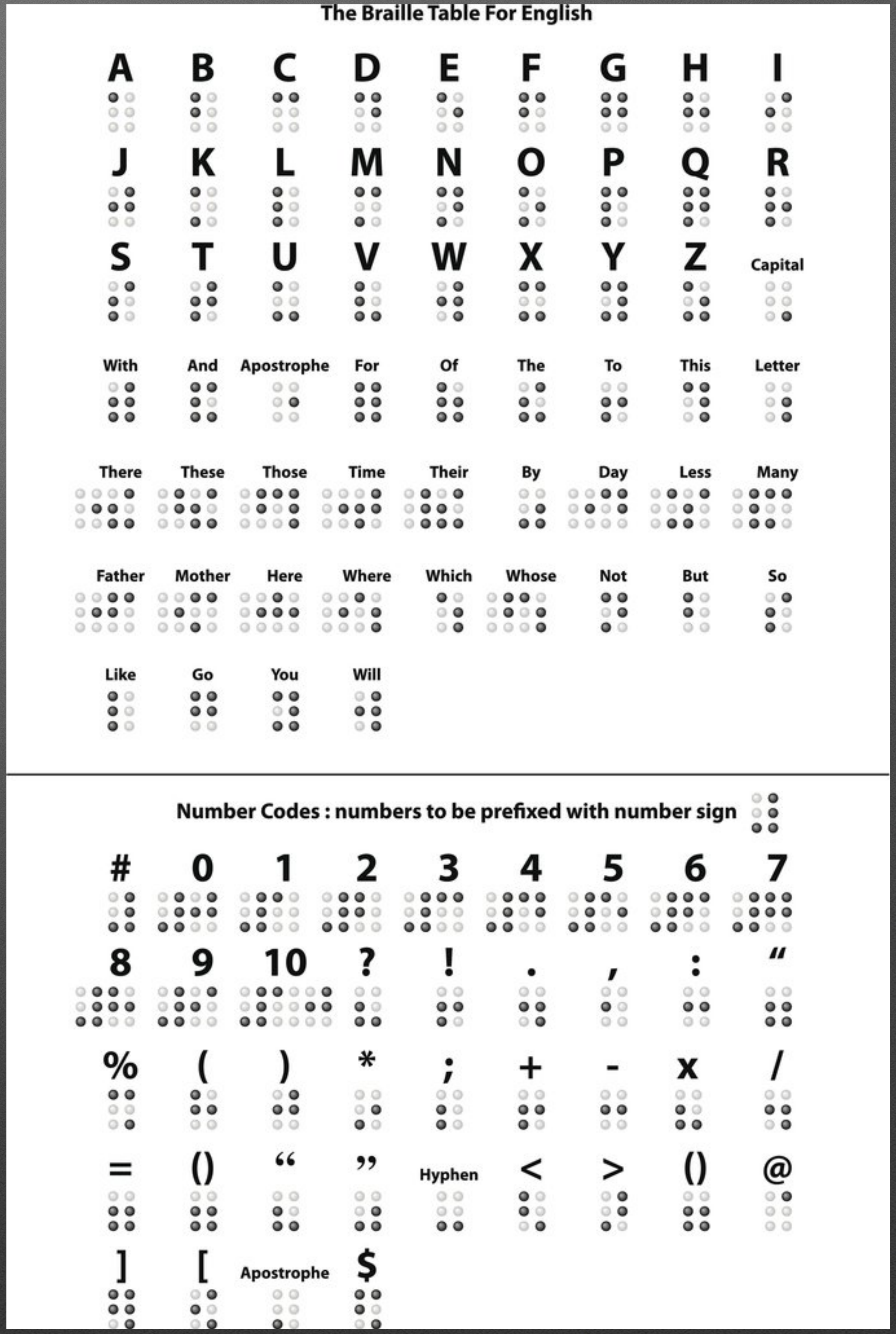
Hashing

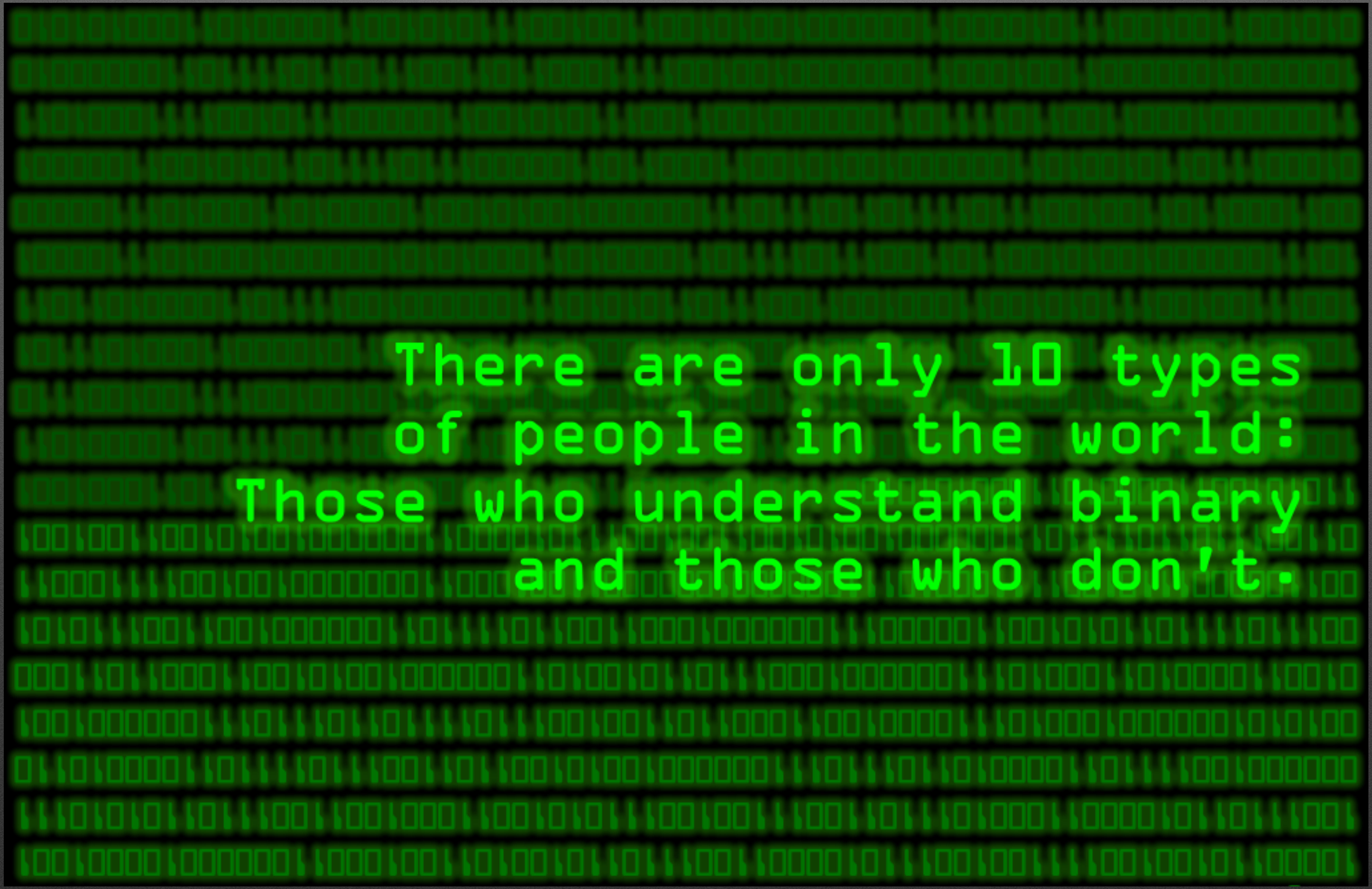

Fox
Hash function
DFCD3454
The red fox runs across the ice
Hash function
52ED879E
The red fox walks across the ice
Hash function
46042841

Secure Hash Algorithm — SHA

Encryption != Encoding


American (Morse)
Continental (Gerke)
International (ITU)
A Ä B C CH D E F G H I J K L M N O Ö P Q R S T U Ü V W X Y Z
1 2 3 4 5 6 7 8 9 0 0 (alt)


The Braille Table For English
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 Capital
With And Apostrophe For Of The To This Letter
There These Those Time Their By Day Less Many
Father Mother Here Where Which Whose Not But So
Like Go You Will
Number Codes : numbers to be prefixed with number sign
0 1 2 3 4 5 6 7
8 9 10 ? ! . , : “
% ( ) * ; + - x /
= () “ ” Hyphen < > () @
] [Apostrophe $


There are only 10 types
of people in the world:
Those who understand binary
and those who don't.

01100010 01101001 01110100 01110011

Table of Number Systems

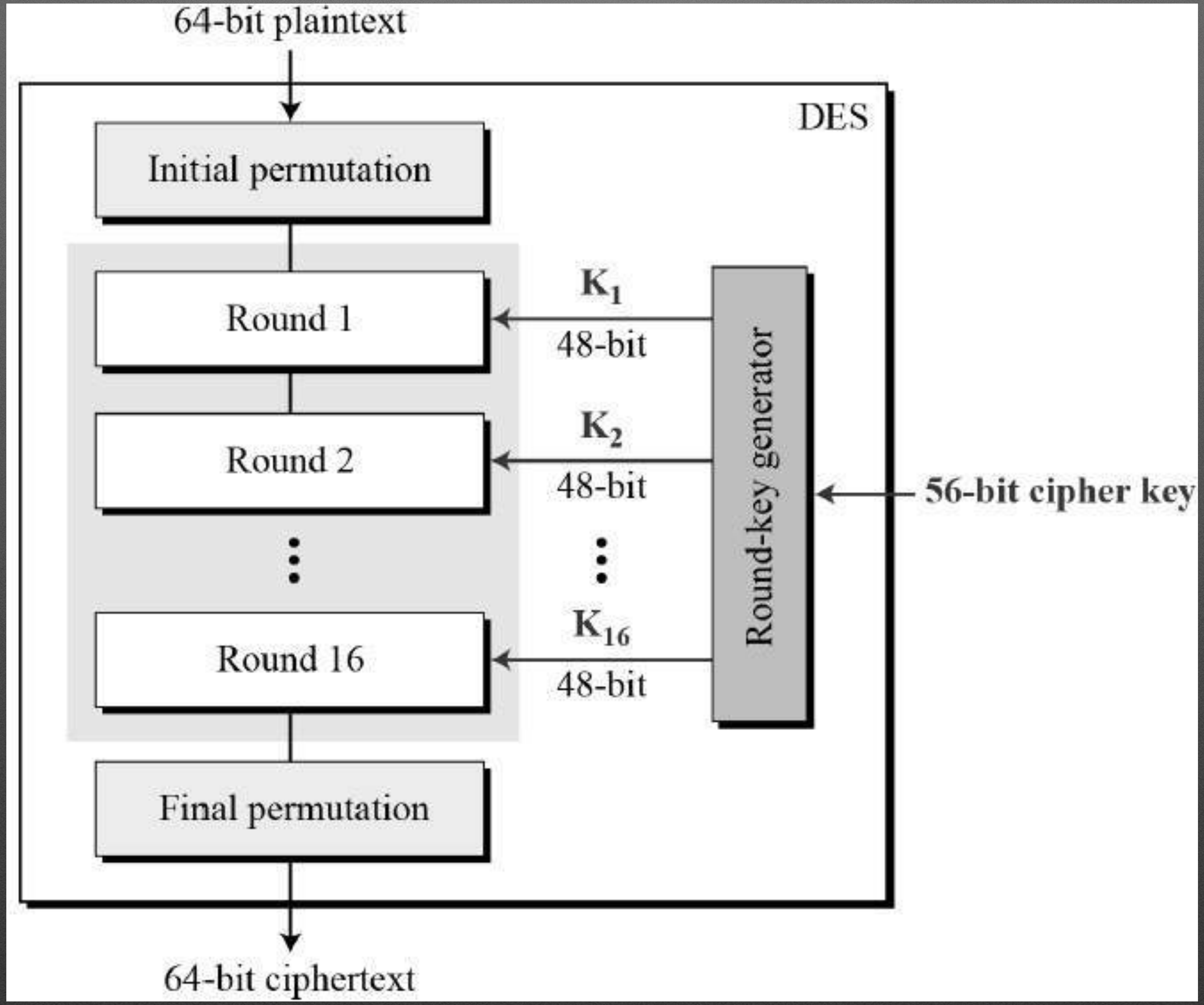
DECIMAL	BINARY	HEXADECIMAL	OCTAL
0	0000	0	0
1	0001	1	1
2	0010	2	2
3	0011	3	3
4	0100	4	4
5	0101	5	5
6	0110	6	6
7	0111	7	7
8	1000	8	10
9	1001	9	11
10	1010	A	12
11	1011	B	13
12	1100	C	14
13	1101	D	15
14	1110	E	16
15	1111	F	17

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

01100010	01101001	01110100	01110011
b	i	t	s

Data Encryption Standard — DES



https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening 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.**

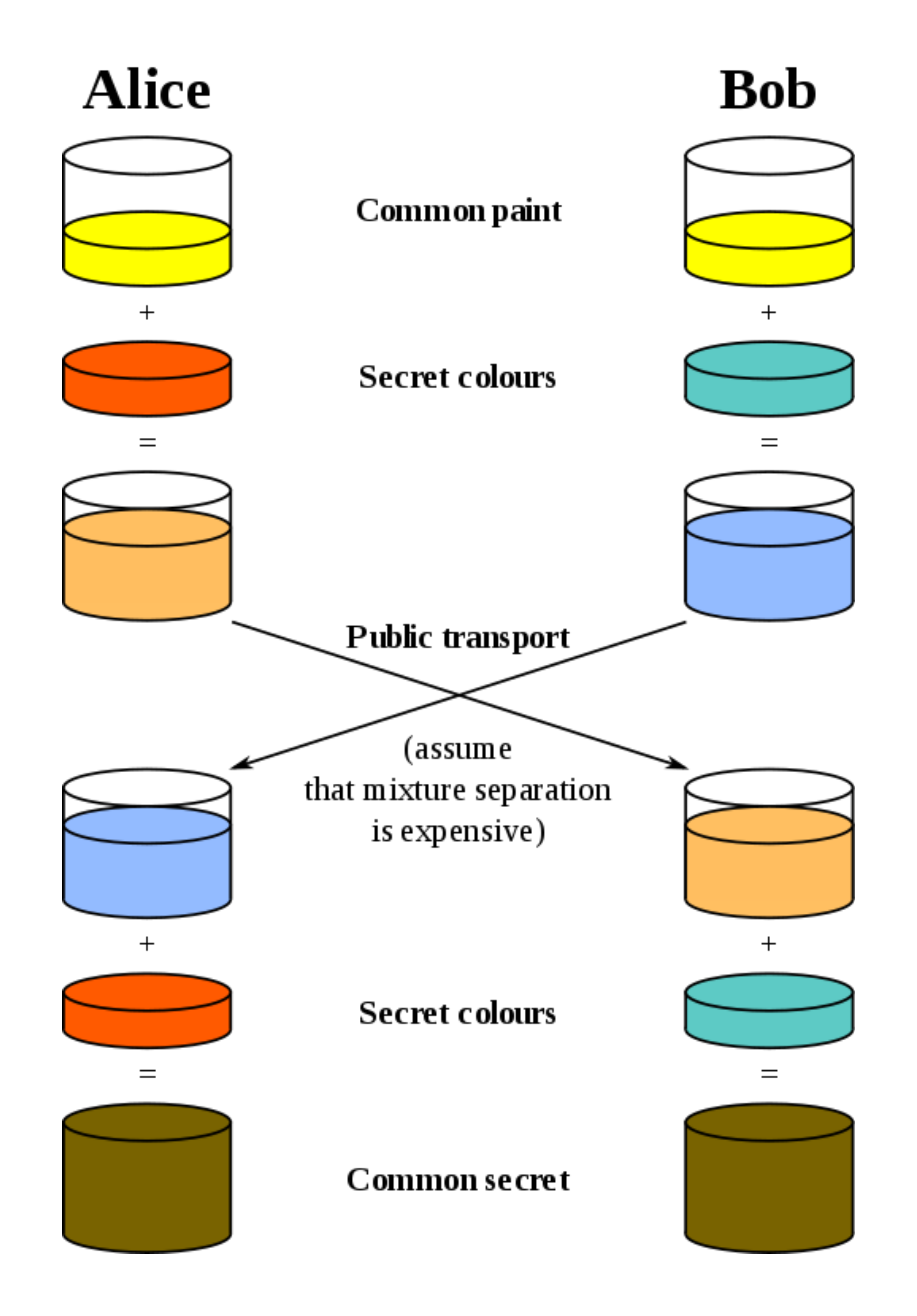
I. Introduction

WE STAND 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 and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

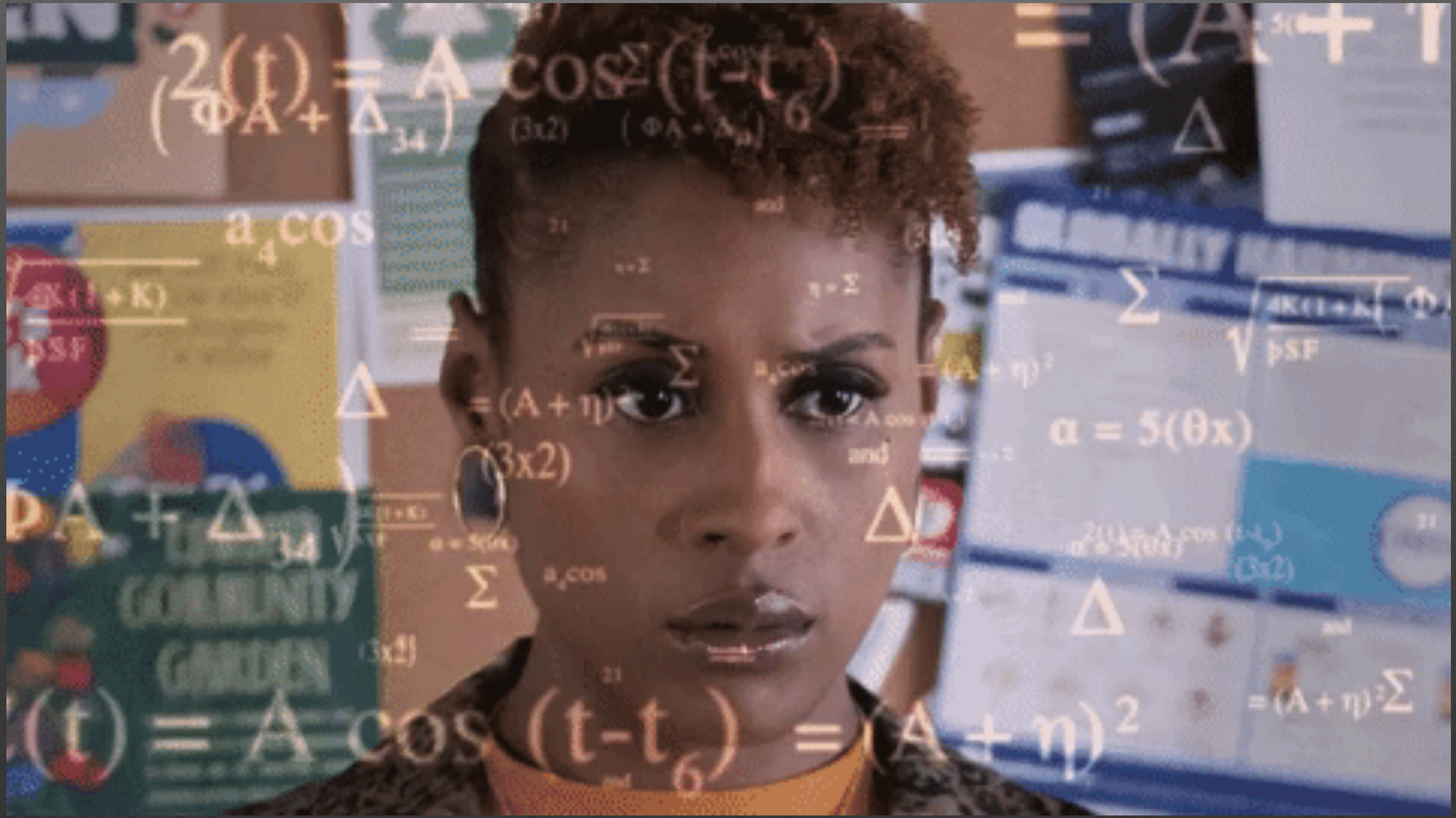
The development of computer controlled communica-

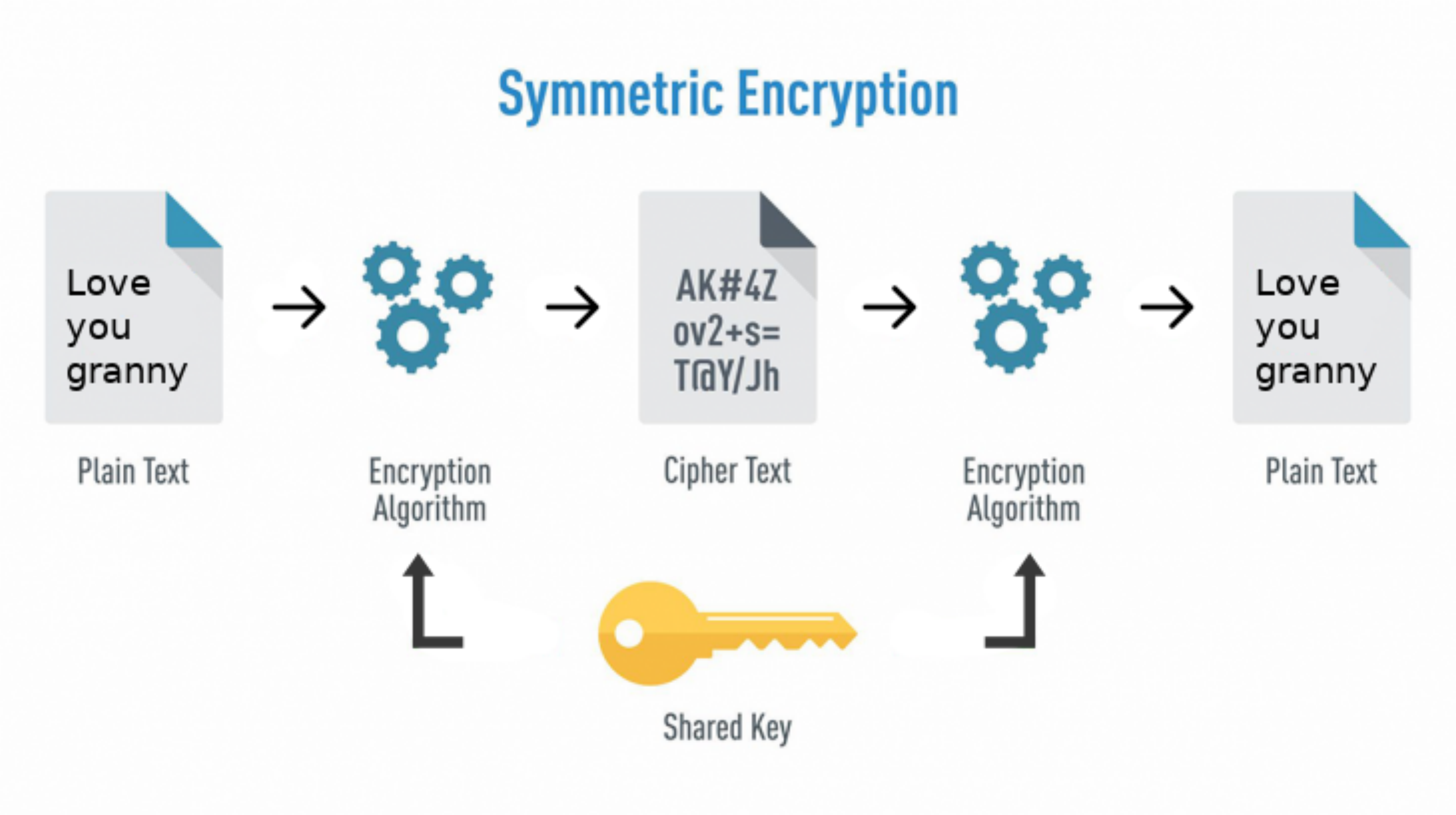
The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to 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 III 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 key D. Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enciphered in such a way that only the intended receiver is able

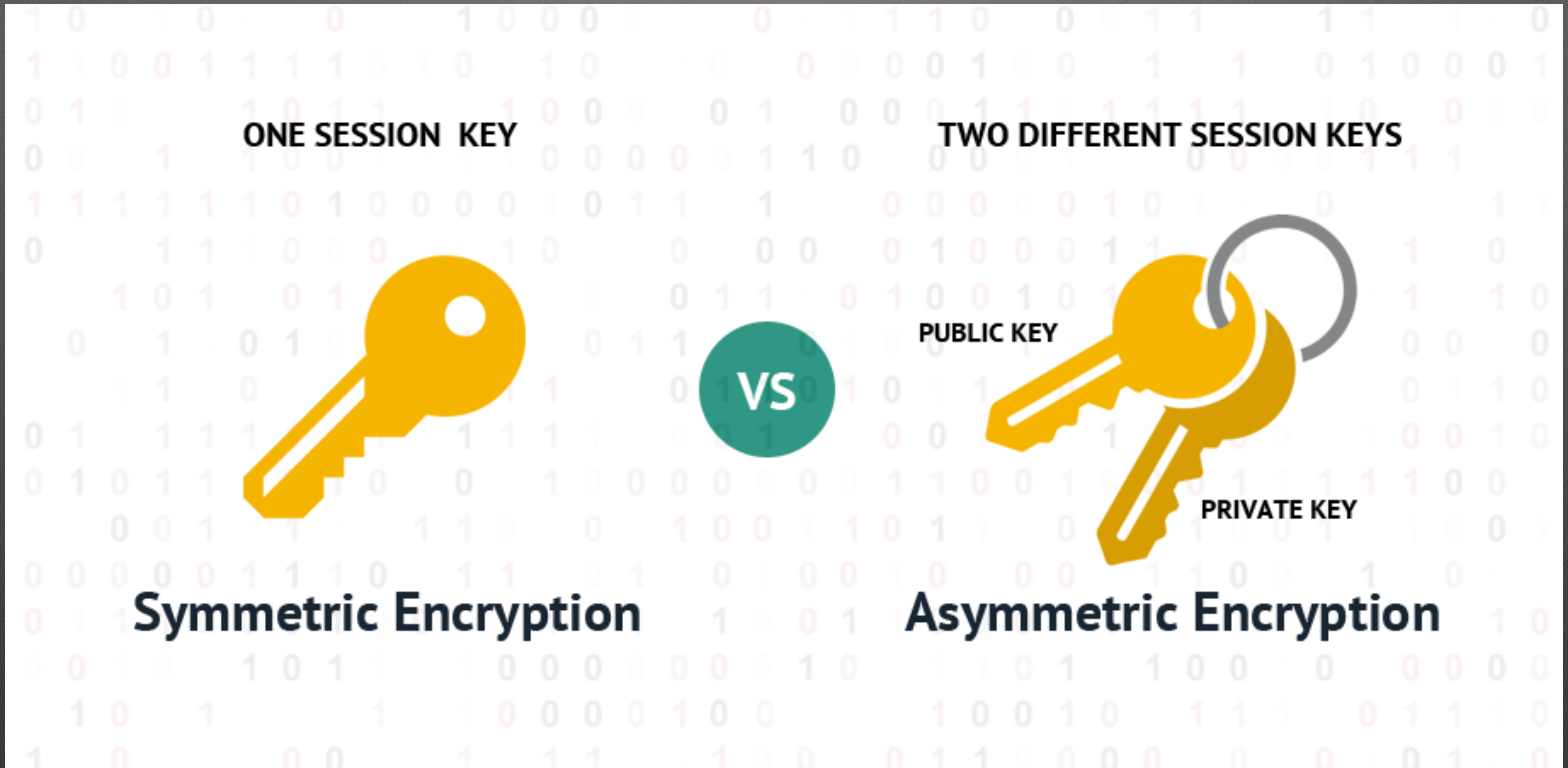

Alice
Bob
Common paint
+
Secret colours
=
Public transport
(assume
that mixture separation
is expensive)
+
Secret colours
=
Common secret

Everything is Math



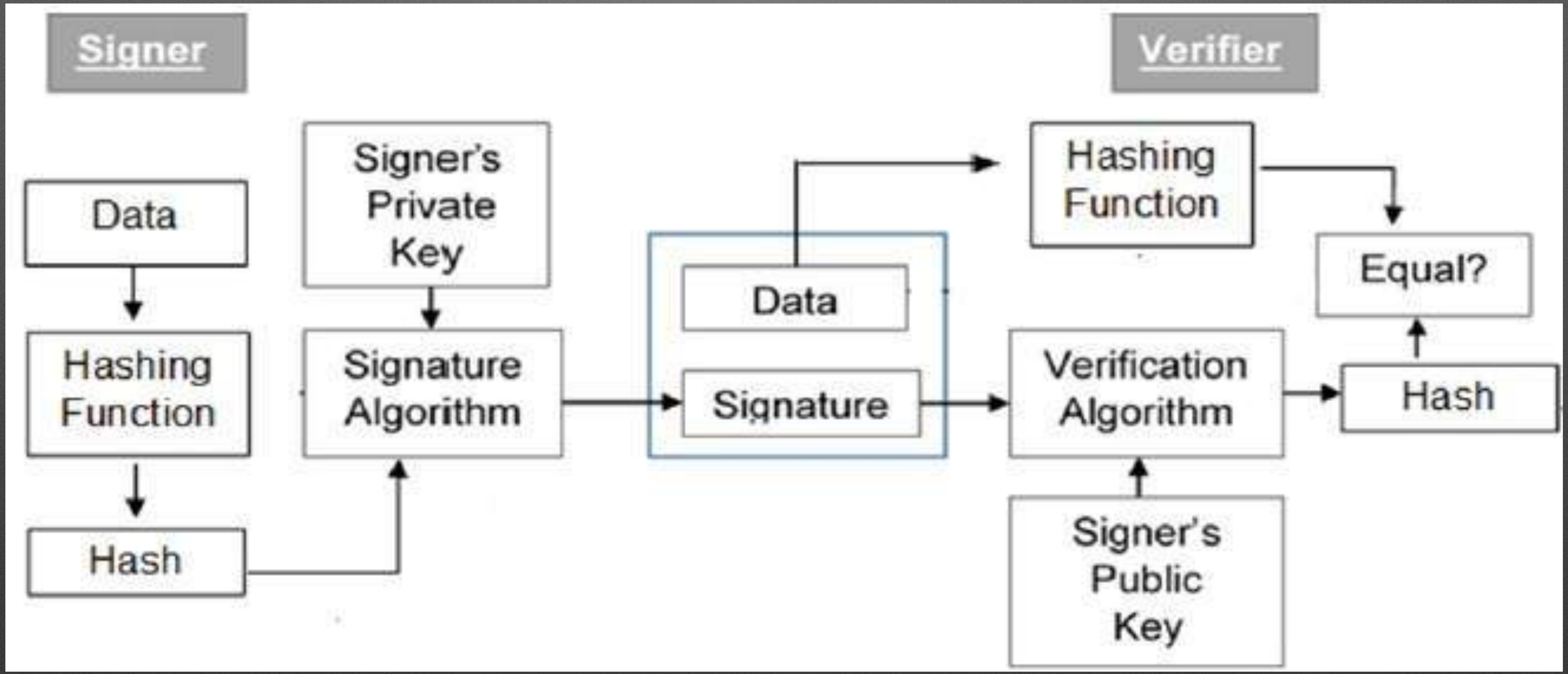


https://hackernoon.com/symmetric-and-asymmetric-encryption-5122f9ec65b1



https://www.cheapsslshop.com/blog/demystifying-symmetric-and-asymmetric-methods-of-encryption

Digital Signatures



https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm

RSA Algorithm

Key Generation

Select p,q	p and q both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e,n\}$
Private key	$KR = \{d,n\}$

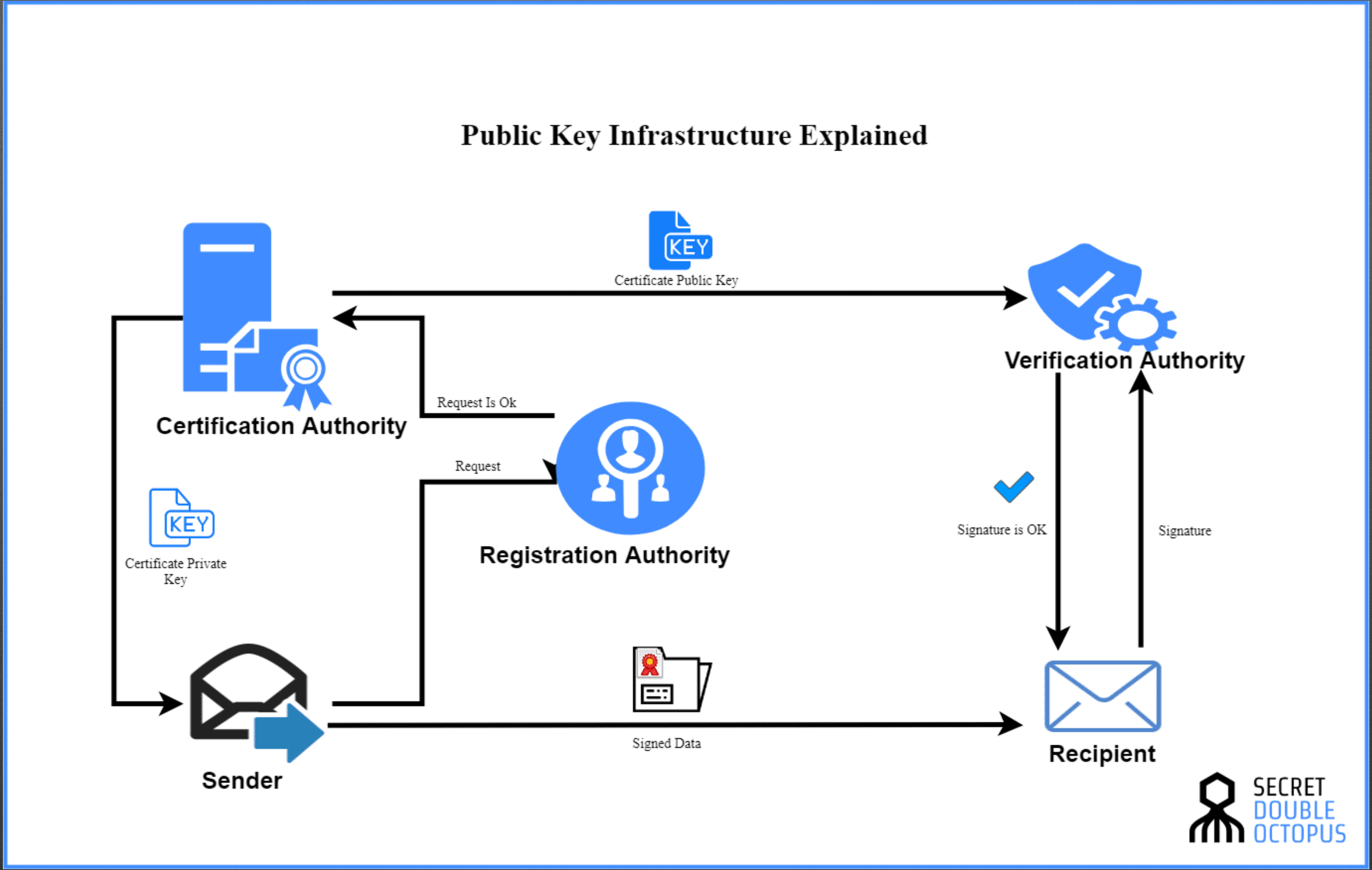
Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption

Plaintext:	C
Ciphertext:	$M = C^d \pmod{n}$

https://kifanga.com/what-is-rsa-algorithm/



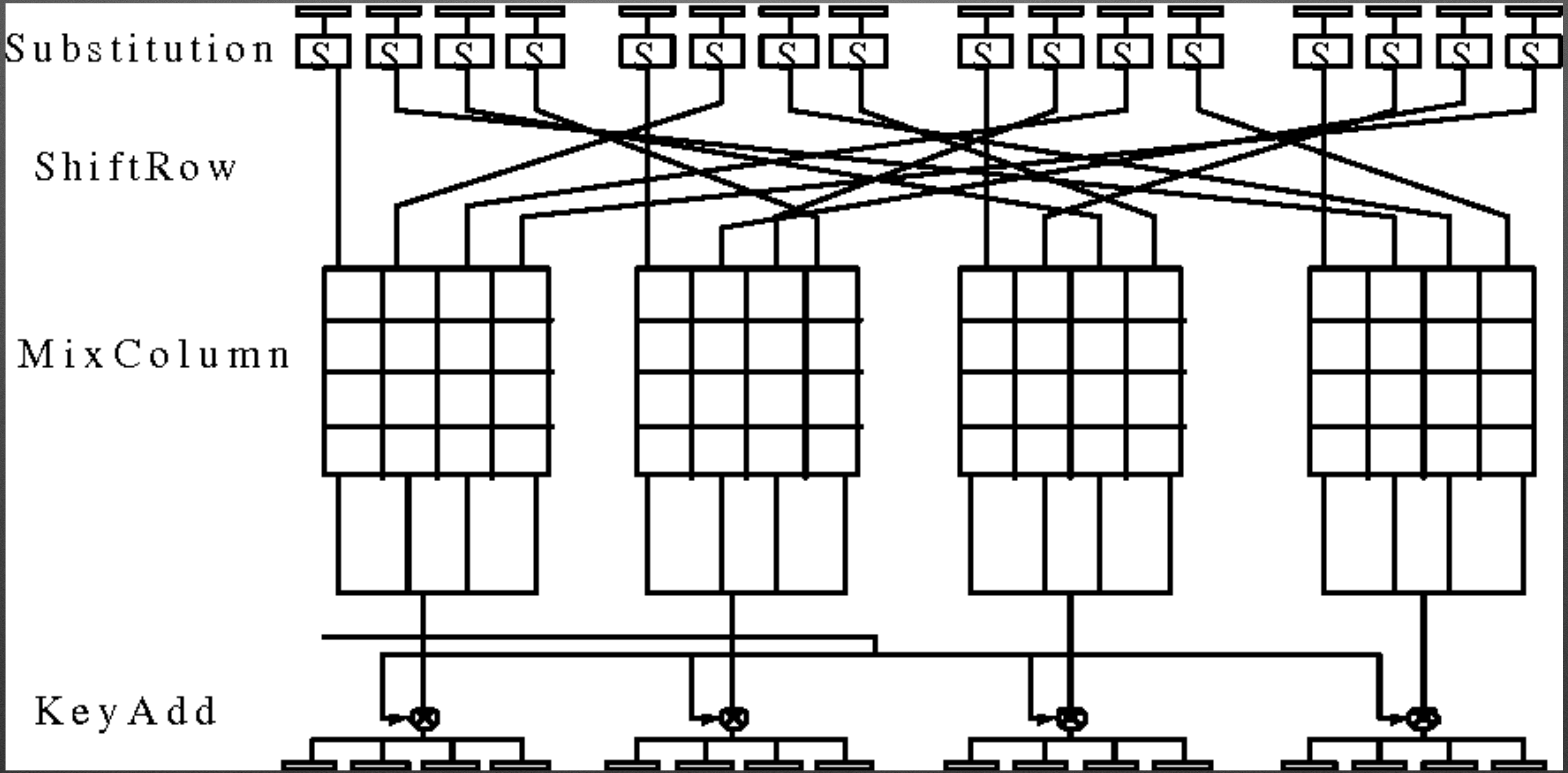
https://doubleoctopus.com/security-wiki/digital-certificates/public-key-infrastructure/

Public Key Encryption

- Secure email
- Desktop security
- Web-based security
- E-commerce
- Access control
- Virtual private networks
- Digital Signatures

Advanced Encryption Standard — AES

Rijndael

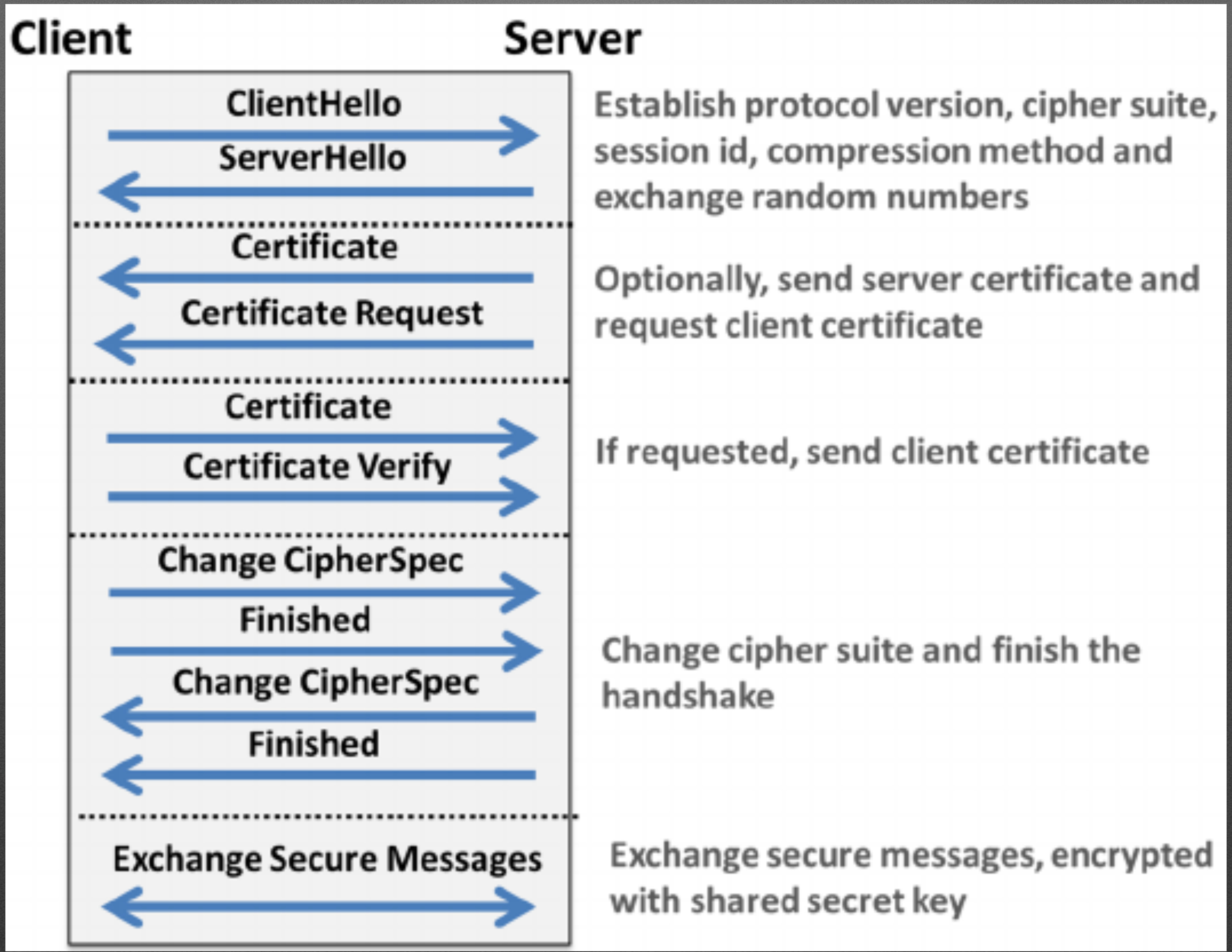


https://link.springer.com/chapter/10.1007%2F3-540-44709-1_6

Symmetric Encryption

- Payment Applications
- Secure File Transfer Protocols
  - FTPS, HTTPS, SFTP, etc.
- Files and File Systems
- Archive and Compression Tools

Transport Layer Security



https://www.researchgate.net/figure/Overview-of-the-Transport-Layer-Security-TLS-Protocol_fig4_272079845

Data in Motion

Vs.

Data at Rest

The Future of Encryption

Thank you!