CRYPTOGRAPHY

Murat Osmanoglu

CRYPTOGRAPHY

"Kryptós" + "gráphein"

secret writing

CRYPTOGRAPHY

"Kryptós" + "gráphein"

secret writing

Cryptography

Cryptanalysis

CRYPTOGRAPHY

"Kryptós" + "gráphein"

secret writing

Cryptography study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks

Cryptanalysis the study of defeating and strengthening cryptographic techniques; that is, finding, exploiting, and correcting weaknesses in either the algorithms themselves or in particular implementations

CRYPTOGRAPHY

"Kryptós" + "gráphein"

secret writing

Cryptography study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks

how to use ciphers to encrypt and decrypt information

Cryptanalysis the study of defeating and strengthening cryptographic techniques; that is, finding, exploiting, and correcting weaknesses in either the algorithms themselves or in particular implementations

how to break ciphers

CRYPTOGRAPHY

"Kryptós" + "gráphein"

secret writing

Cryptography study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks

how to use ciphers to encrypt and decrypt information

+

Cryptanalysis the study of defeating and strengthening cryptographic techniques; that is, finding, exploiting, and correcting weaknesses in either the algorithms themselves or in particular implementations

how to break ciphers

=

Cryptology

Designing a Security Protocol

- rigorous definitions of what it means to have secure encryption, signatures, authentication

Designing a Security Protocol

- rigorous definitions of what it means to have secure encryption, signatures, authentication
  - Objective
  - Resources
  - Threat Model
  - Algorithm
  - Assumption

Designing a Security Protocol

- define an Objective that you would like to achieve
  - designing a ledger that blockchain protocol is used to construct
  - designing an unforgeable digital signature scheme

Designing a Security Protocol

- define an Objective that you would like to achieve
  - designing a ledger that blockchain protocol is used to construct
  - designing an unforgeable digital signature scheme
- analyze the Resources that are available to the parties which are using the algorithm to meet the objective

Designing a Security Protocol

- define an Objective that you would like to achieve
  - designing a ledger that blockchain protocol is used to construct
  - designing an unforgeable digital signature scheme
- analyze the Resources that are available to the parties which are using the algorithm to meet the objective
- design the Threat Model to describe what the adversary is allowed to do and what it is not allowed to do

Designing a Security Protocol

- define an Objective that you would like to achieve
  - designing a ledger that blockchain protocol is used to construct
  - designing an unforgeable digital signature scheme
- analyze the Resources that are available to the parties which are using the algorithm to meet the objective
- design the Threat Model to describe what the adversary is allowed to do and what it is not allowed to do
  - to have a good threat model, think exactly what will happen when the algorithm are being executed in the real world (it should reflect the real-time scenario)

Threat Model

- have you considered all possible attackers?

Threat Model

- have you considered all possible attackers?
  - what do they want?
  - why do they want it?
  - what do they have?

Threat Model

- have you considered all possible attackers?
  - what do they want?
  - why do they want it?
  - what do they have?

- have you considered all possible attack surfaces?

Threat Model

- have you considered all possible attackers?
  - what do they want?
  - why do they want it?
  - what do they have?

- have you considered all possible attack surfaces?
  - is the network secure?
  - is the OS secure?
  - is the hardware secure?

Designing a Security Protocol

- design the Algorithm (or Protocol) that uses the available resources, and achieves the objective given the threat model
  - formally prove that this is true!

Designing a Security Protocol

- design the Algorithm (or Protocol) that uses the available resources, and achieves the objective given the threat model
  - formally prove that this is true!
- find a proper Assumption, difficult to solve, that is used when we argue that the algorithm achieves the objective

Designing a Security Protocol

- design the Algorithm (or Protocol) that uses the available resources, and achieves the objective given the threat model
  - formally prove that this is true!
- find a proper Assumption, difficult to solve, that is used when we argue that the algorithm achieves the objective
  - Factorization problem (RSA)
  - Discrete Log Problem (ECDSA)

Designing a Security Protocol

- design the Algorithm (or Protocol) that uses the available resources, and achieves the objective given the threat model
  - formally prove that this is true!
- find a proper Assumption, difficult to solve, that is used when we argue that the algorithm achieves the objective

establish the proof : the algorithm meets the objective given the resources in the threat model we have specified, under the assumption we have described

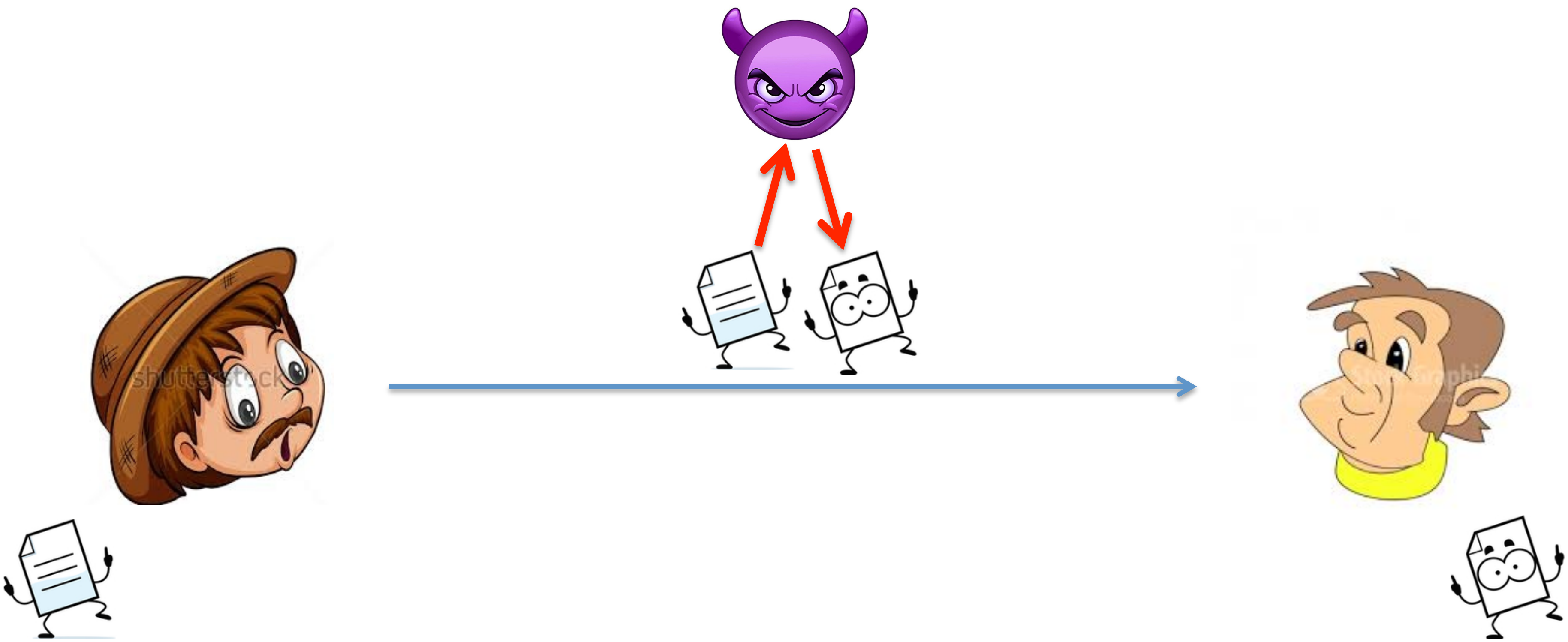
Designing a Security Protocol

- design the Algorithm (or Protocol) that uses the available resources, and achieves the objective given the threat model
  - formally prove that this is true!
- find a proper Assumption, difficult to solve, that is used when we argue that the algorithm achieves the objective

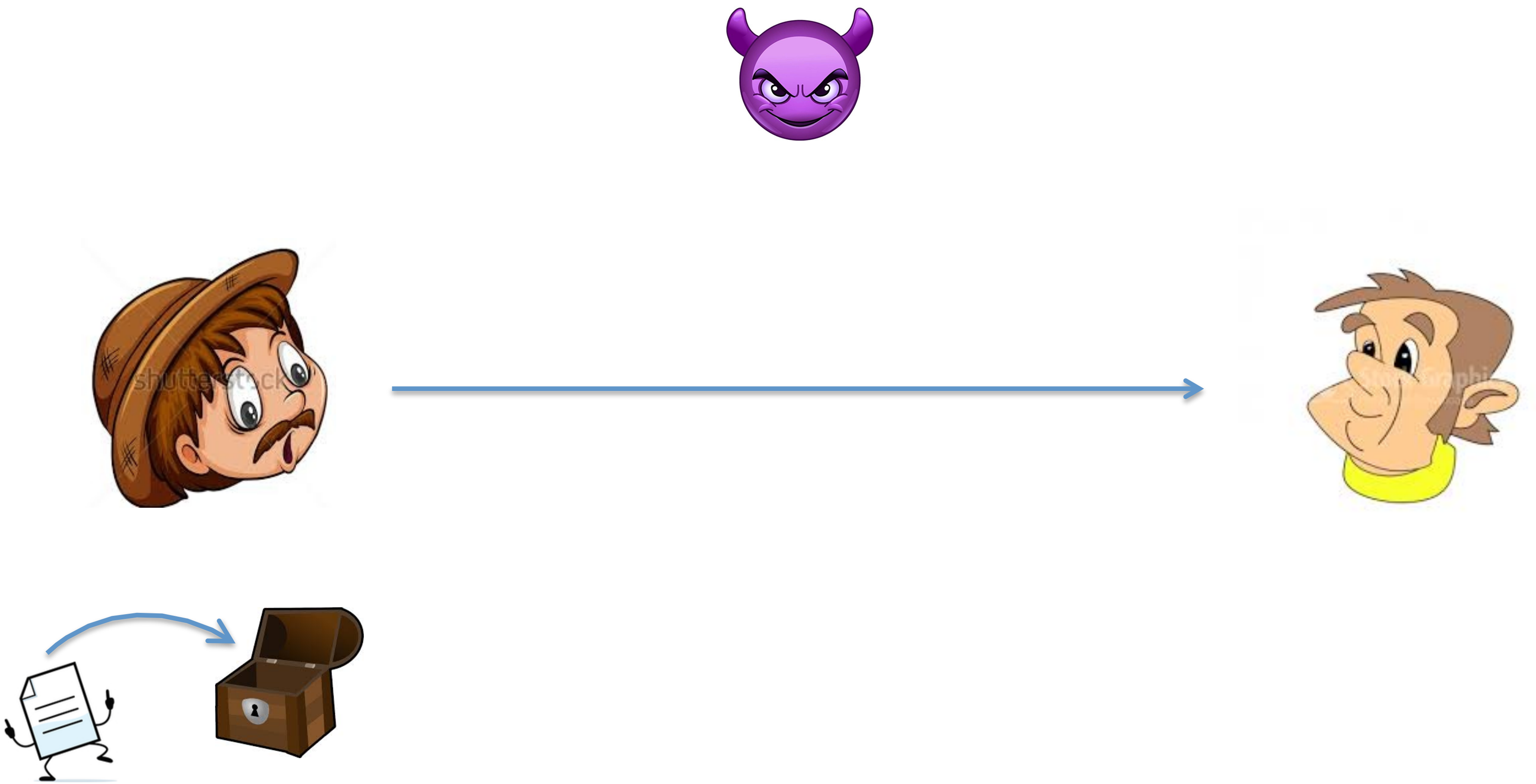
establish the proof : the algorithm meets the objective given the resources in the threat model we have specified, under the assumption we have described

implementation

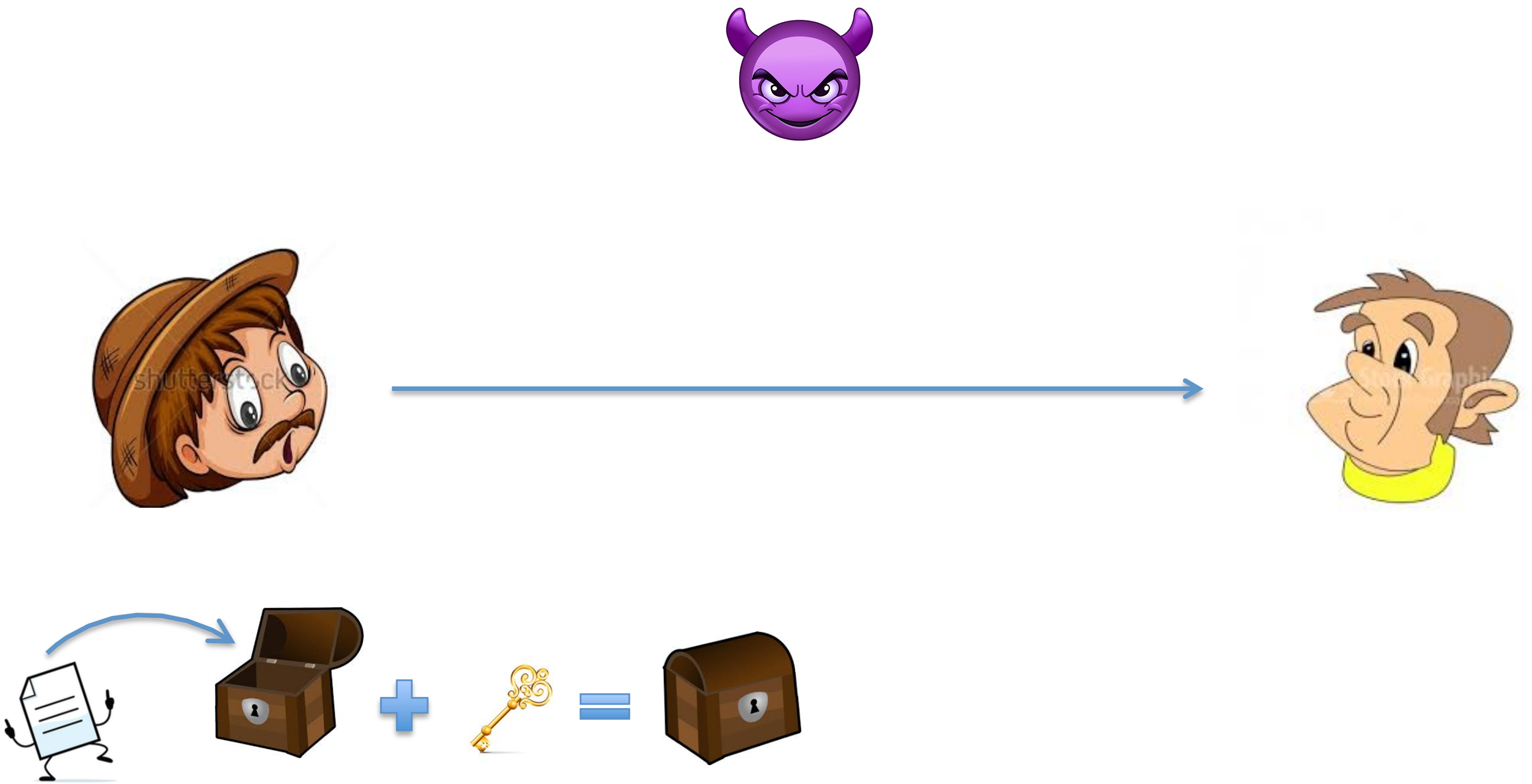
CRYPTOGRAPHY



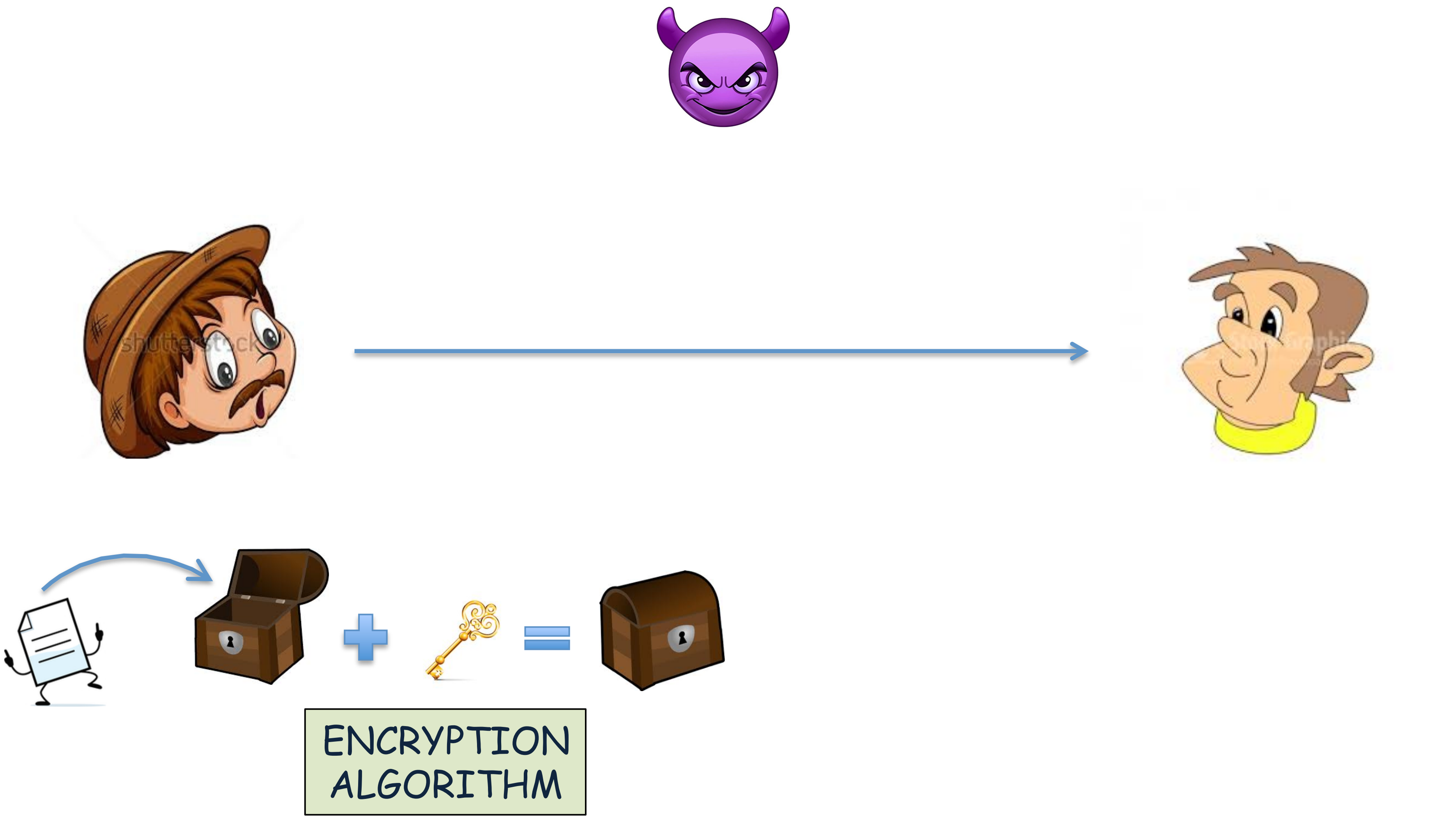
CRYPTOGRAPHY



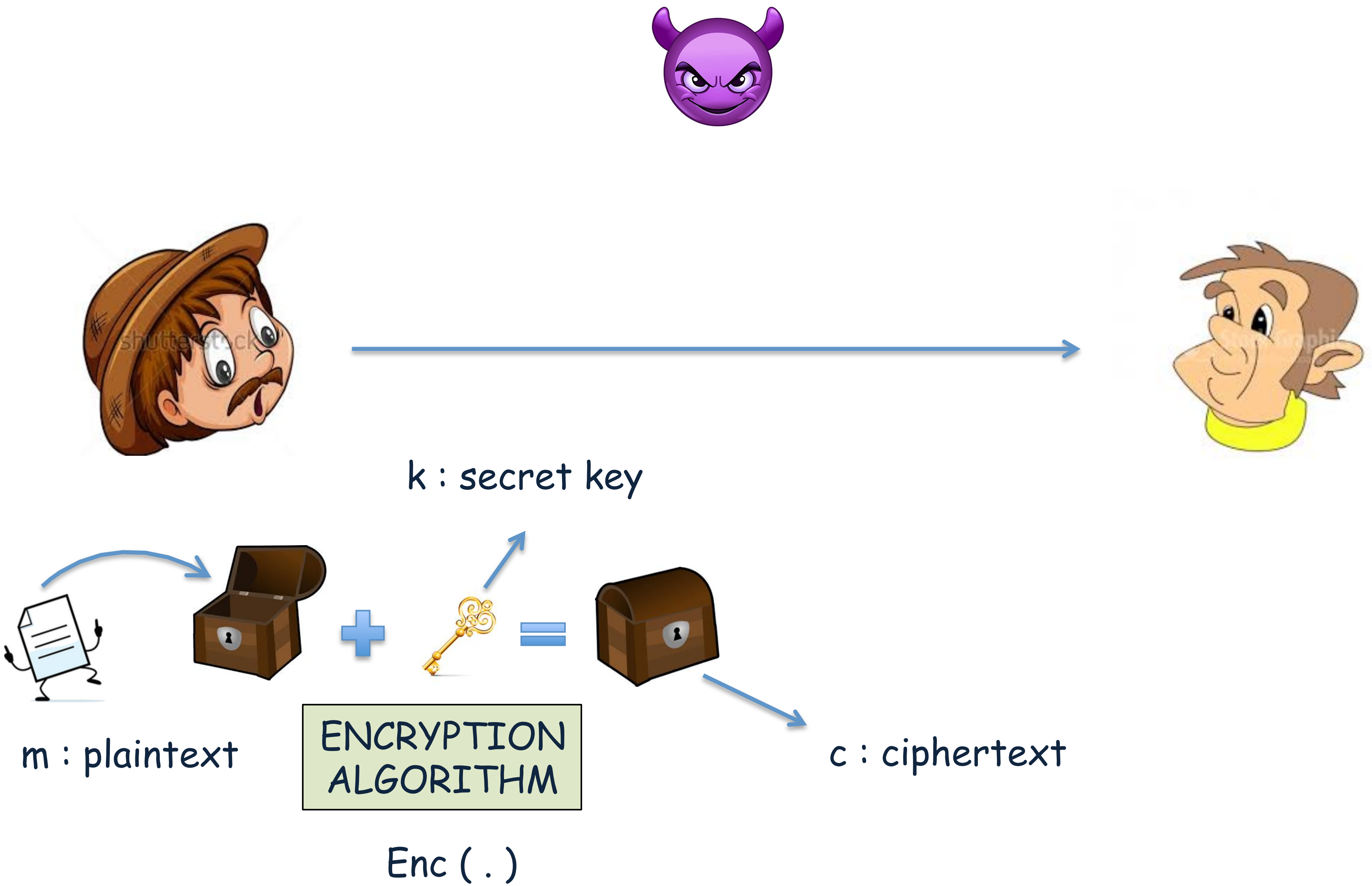
CRYPTOGRAPHY



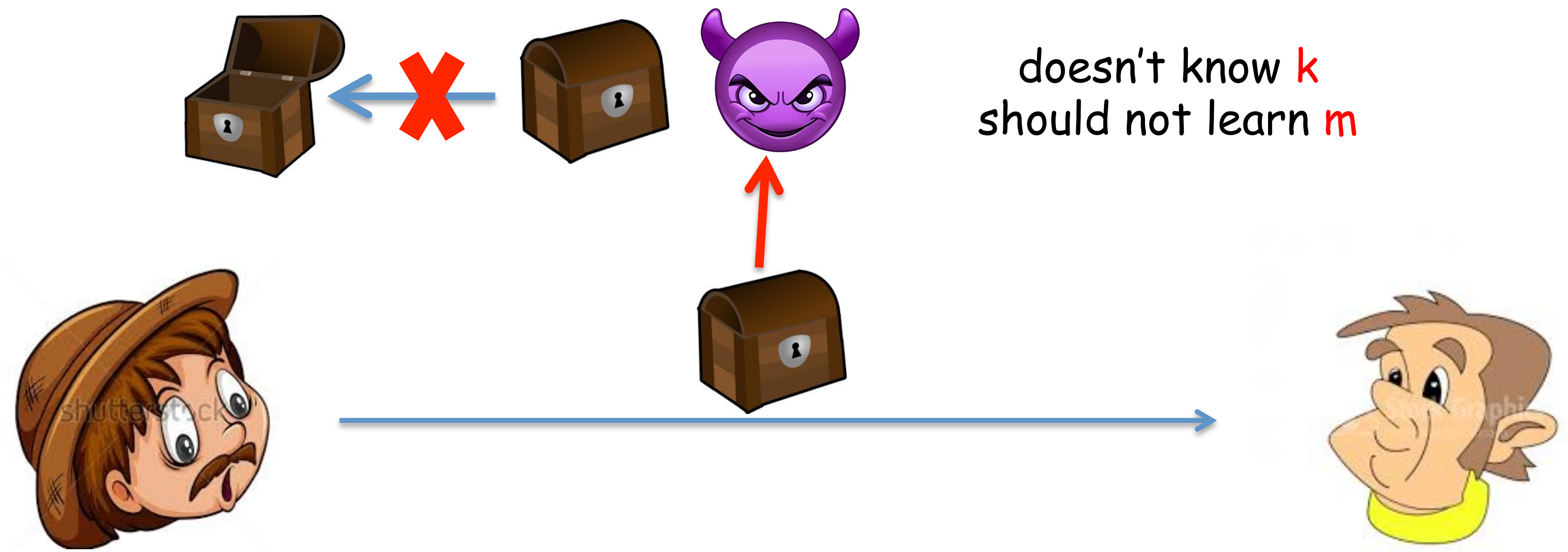
CRYPTOGRAPHY



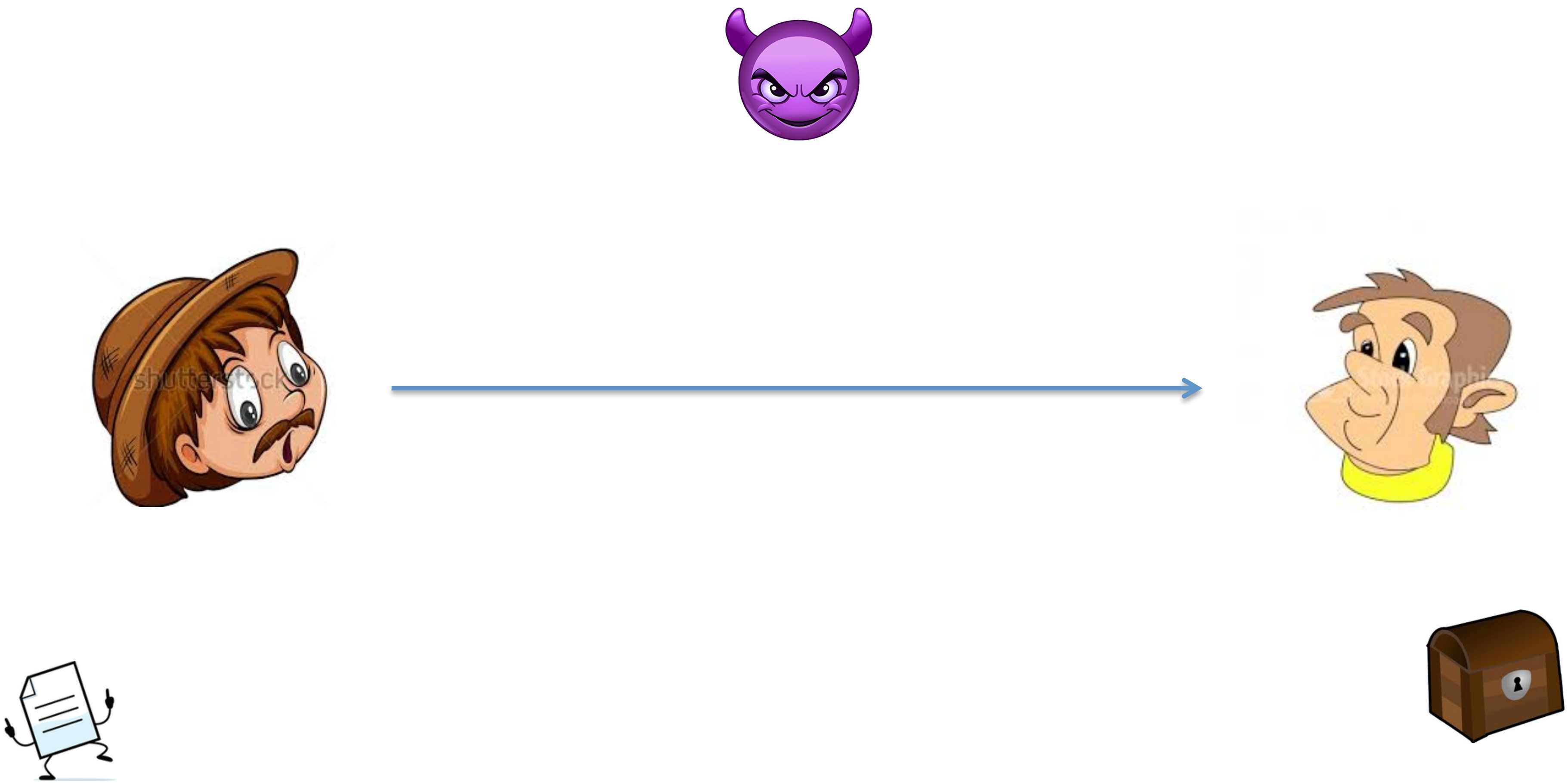
CRYPTOGRAPHY



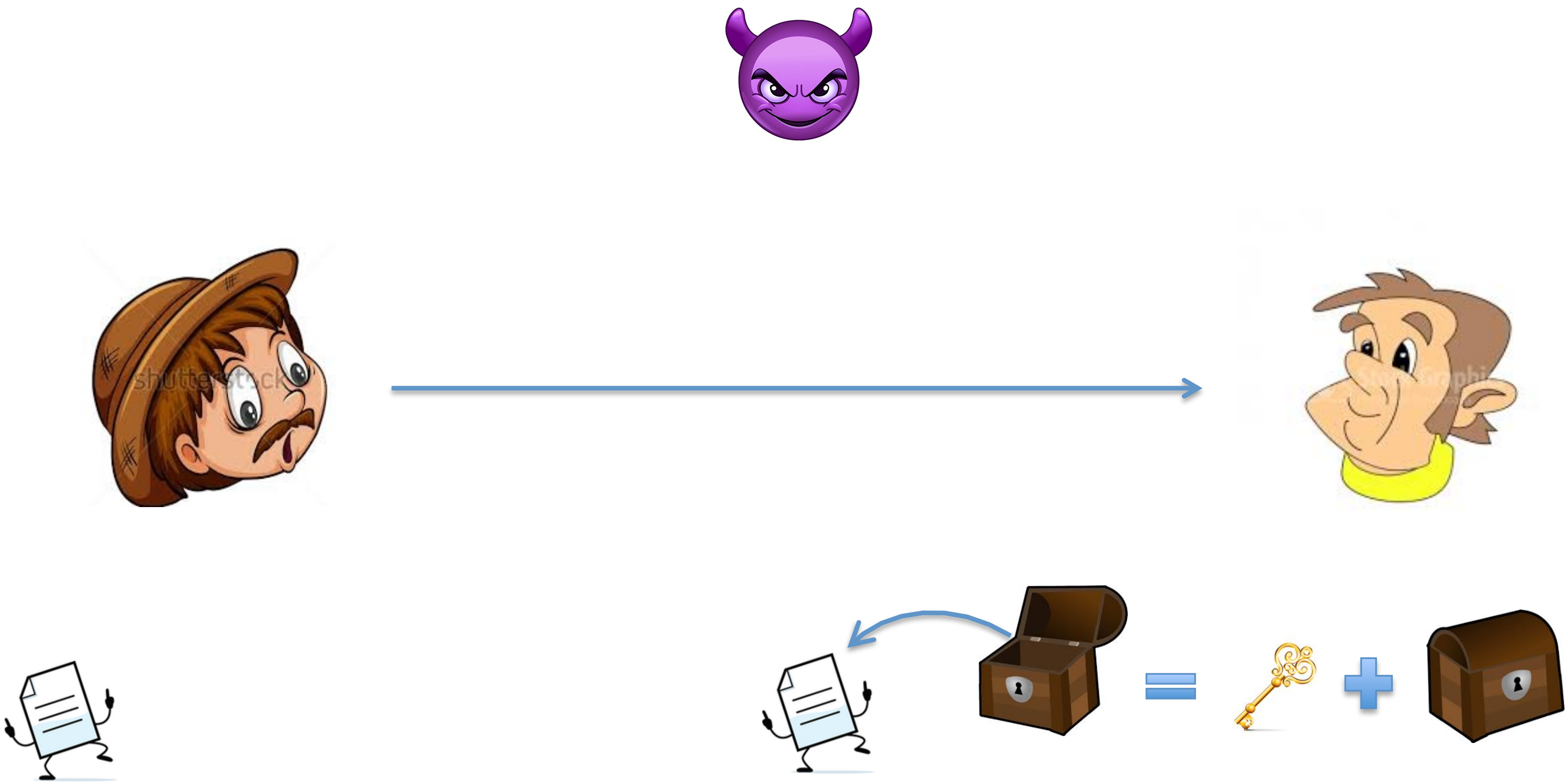
CRYPTOGRAPHY



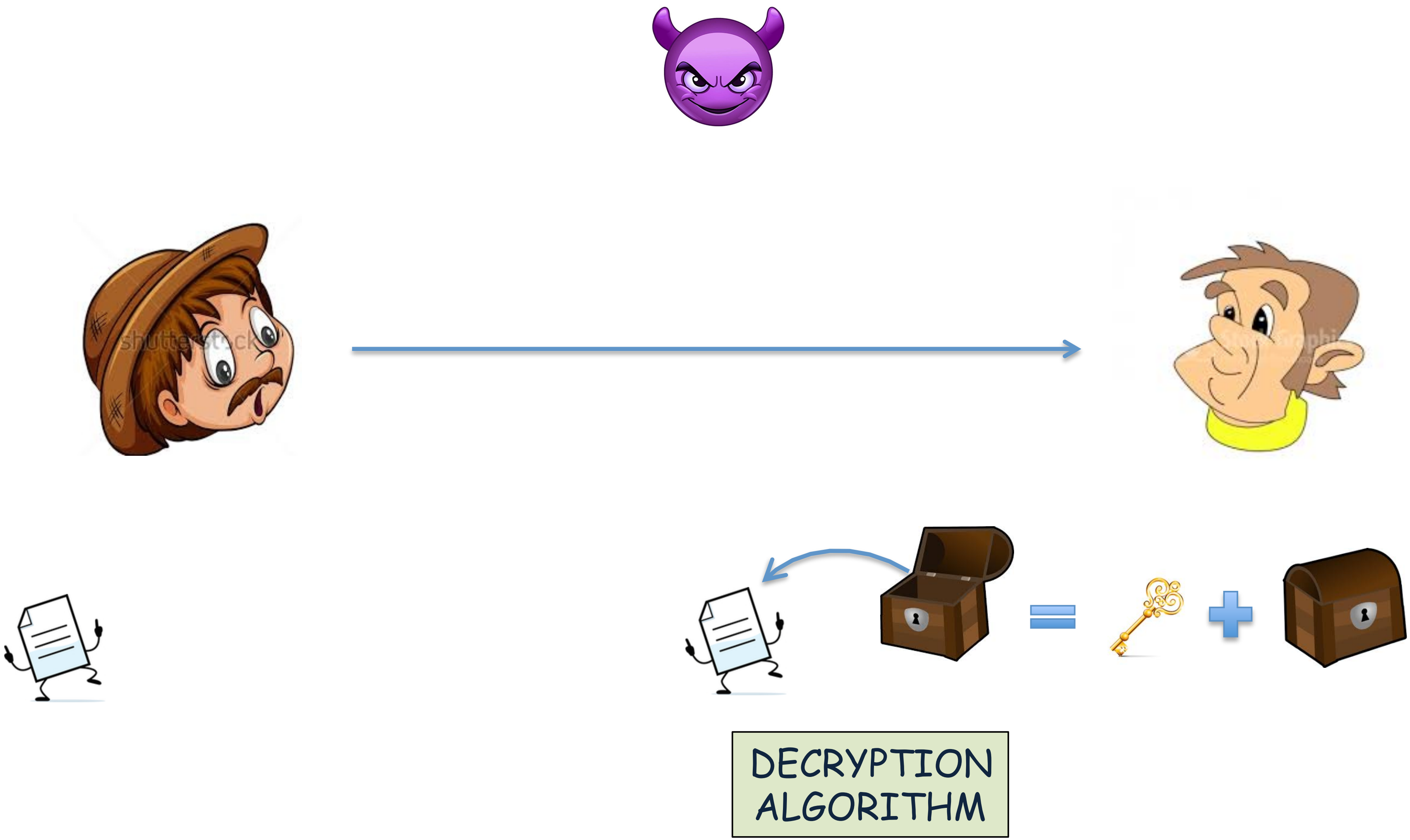
CRYPTOGRAPHY



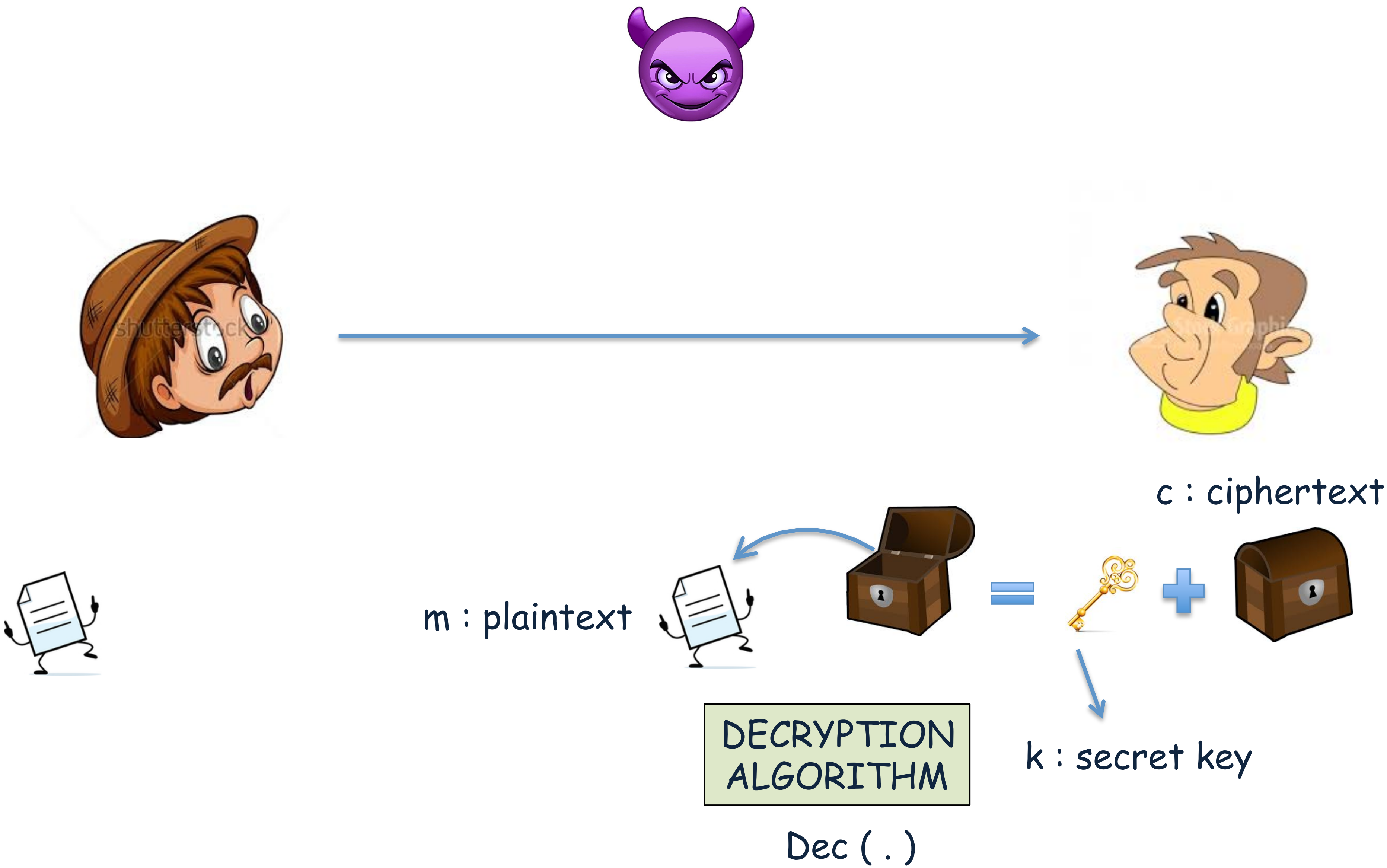
CRYPTOGRAPHY



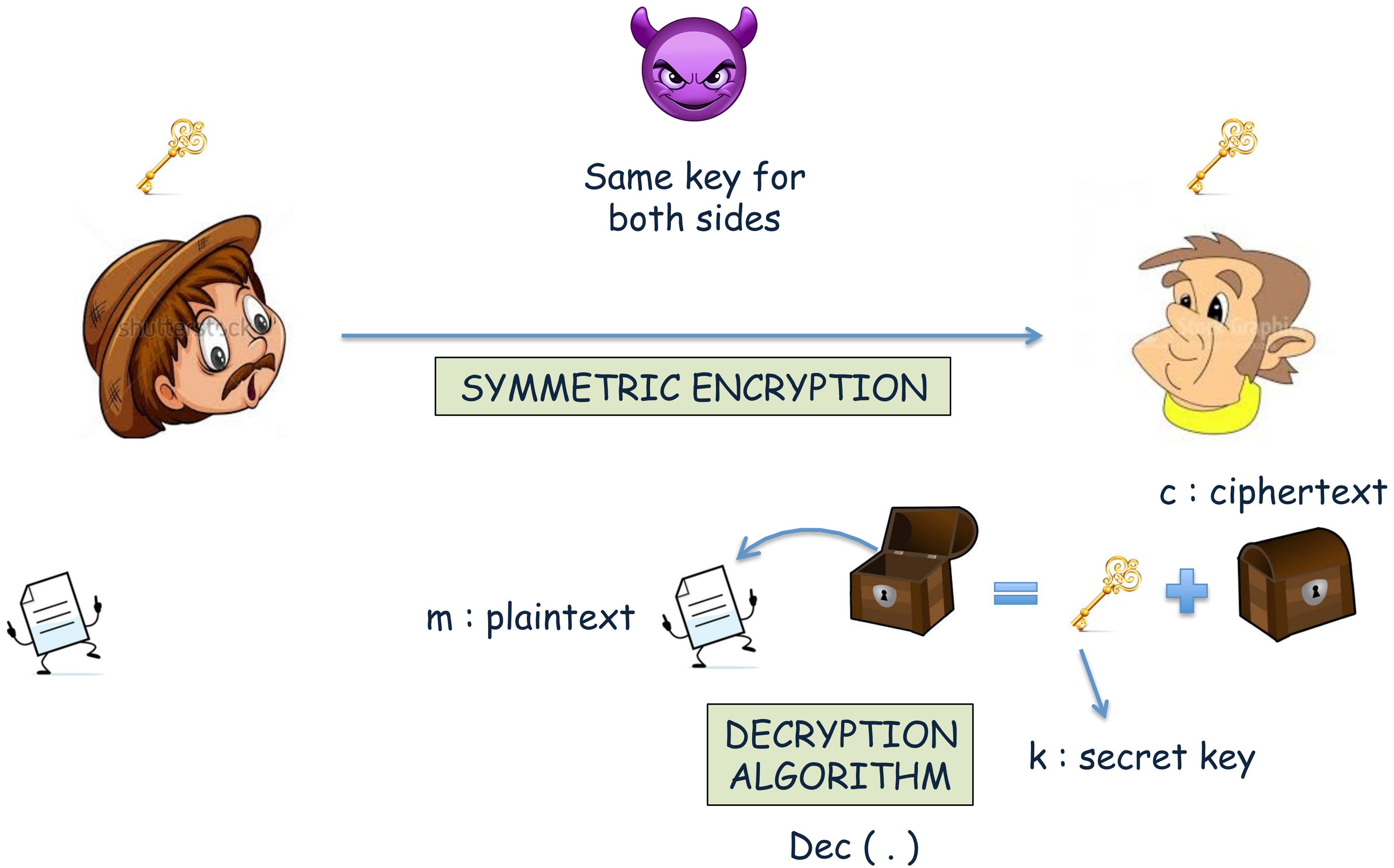
CRYPTOGRAPHY



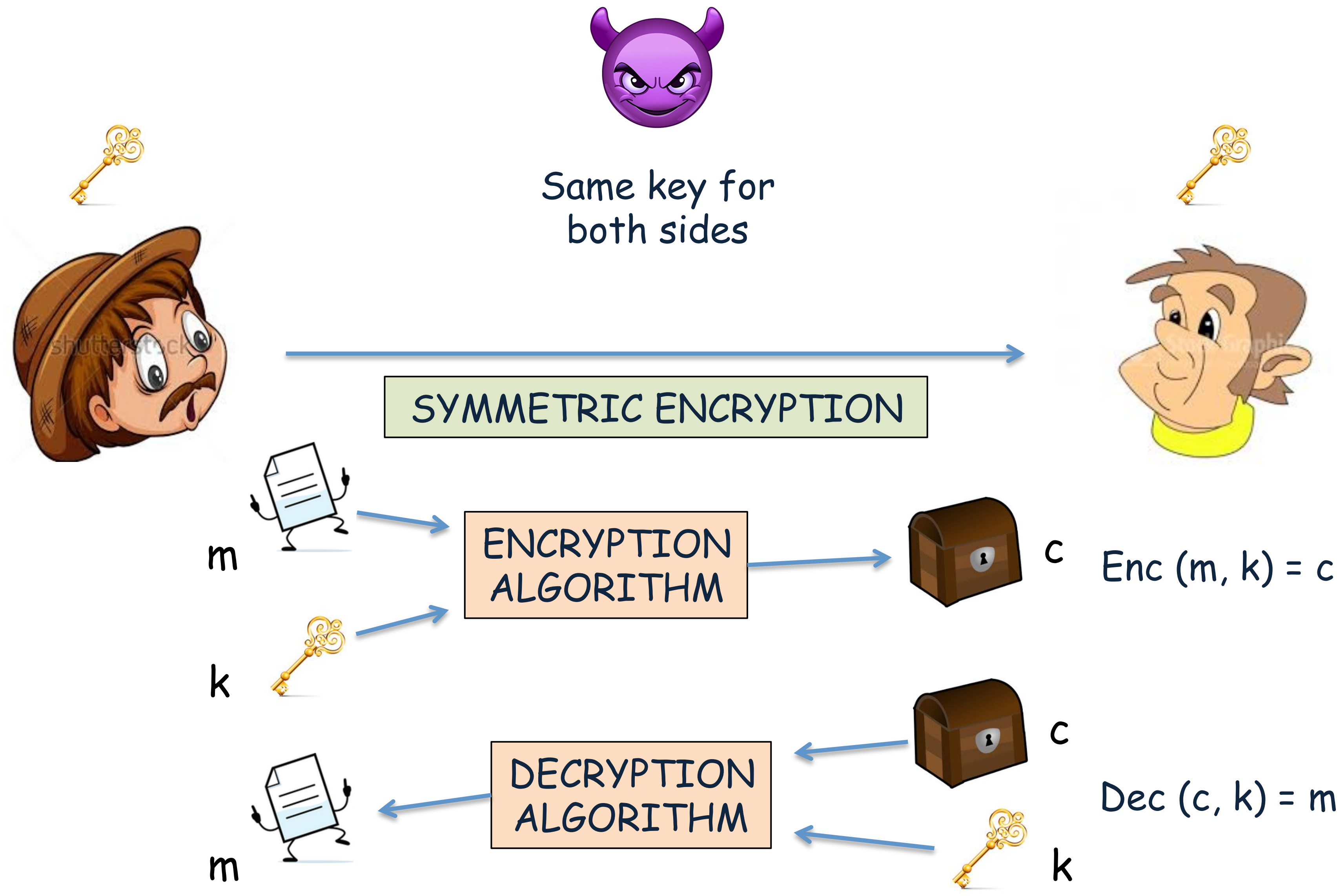
CRYPTOGRAPHY



CRYPTOGRAPHY



CRYPTOGRAPHY



CRYPTOGRAPHY

K : key space M : plaintext space C : ciphertext space

CRYPTOGRAPHY

K : key space   M : plaintext space   C : ciphertext space

An encryption scheme consists of (Gen, Enc, Dec) :

- Gen : N → K is a key generation algorithm
- Enc : K X M → C is an encryption algorithm
- Dec : K X C → M is a decryption algorithm

CRYPTOGRAPHY

K : key space M : plaintext space C : ciphertext space

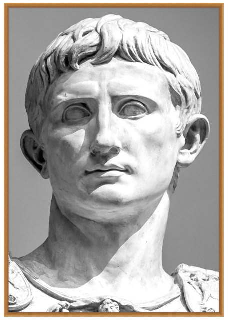
An encryption scheme consists of (Gen, Enc, Dec) :

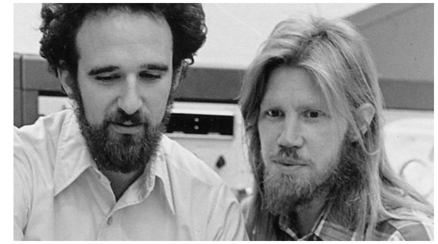
- Gen : N → K is a key generation algorithm
- Enc : K X M → C is an encryption algorithm
- Dec : K X C → M is a decryption algorithm

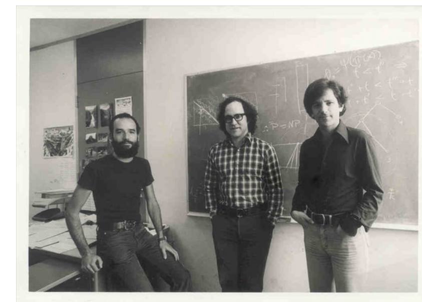
Correctness

For every k and m, we should have Dec (Enc(m, k), k) = m

CRYPTOGRAPHY





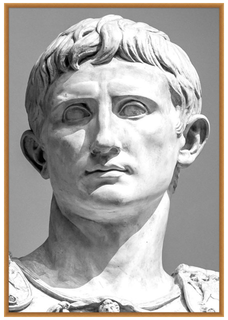


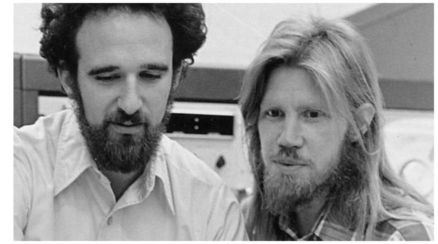
1980s

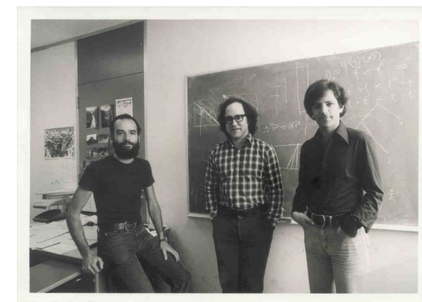
historical cryptography

modern cryptography

CRYPTOGRAPHY





1980s

historical cryptography

- just encryptions
- military and governments
- dealing with constructing good codes, or breaking existing one (no working definition of what constitutes a good code)

modern cryptography

- public-key cryptography, signature schemes, zero-knowledge, crypto currencies, …
- everywhere
- considered as a science and mathematical discipline

Ceasar Cipher

3

3

plaintext ← K L E O P A T R A

\+

secret key ← 3

shift 3 to the right

ciphertext ← N O H R S D W U D

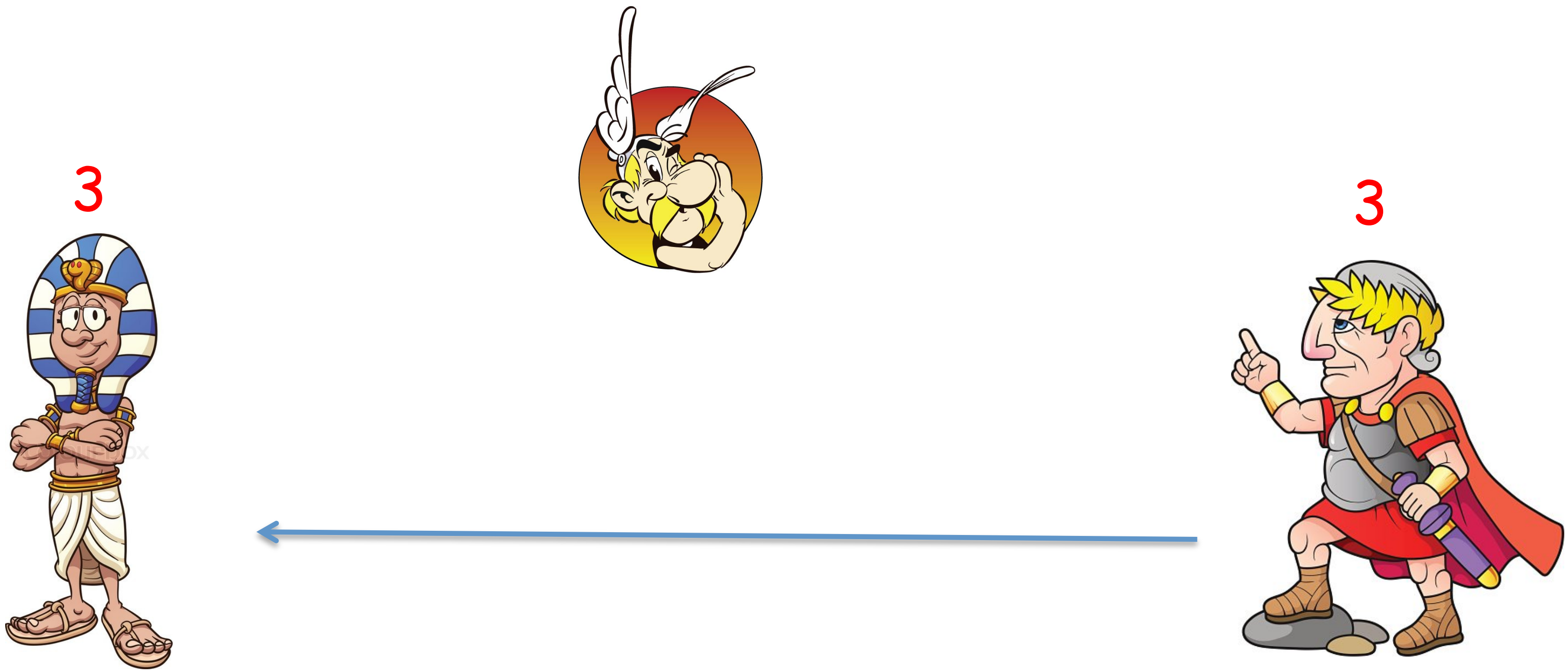
Ceasar Cipher

3

3

NOHRSDWUD

Ceasar Cipher



N O H R S D W U D → ciphertext

−

3 → secret key

shift 3 to the left

C L E O P A T R A → plaintext

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

- The "boss of bosses" of the Sicilian Mafia, Bernardo Provenzano (Binnu u tratturi – Binnu the tractor), used a modified form of the Caesar cipher to obscure "sensitive information" in notes left to either his family or underlings.

C	A	R	L	E	O	N	E
2	0	17	11	4	14	13	4
			+ 3				
5	3	20	14	7	17	16	7

ciphertext

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

K = {0, 1, …, 25}   M = {A, B, …, Z} = {0, 1, …, 25}

Enc(m_1, …, m_n, k) = (m_1 + k mod 26, …, m_n + k mod 26)

Dec(c_1, …, c_n, k) = (c_1 - k mod 26, …, c_n - k mod 26)

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

K = {0, 1, …, 25}   M = {A, B, …, Z} = {0, 1, …, 25}

Enc(m_1, …, m_n, k) = (m_1 + k mod 26, …, m_n + k mod 26)

Dec(c_1, …, c_n, k) = (c_1 - k mod 26, …, c_n - k mod 26)

C	A	R	L	E	O	N	E
2	0	17	11	4	14	13	4

+

15

17	15	6	0	19	3	2	19
R	P	G	A	T	D	C	T

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

K = {0, 1, …, 25}   M = {A, B, …, Z} = {0, 1, …, 25}

Enc(m_1, …, m_n, k) = (m_1 + k mod 26, …, m_n + k mod 26)

Dec(c_1, …, c_n, k) = (c_1 - k mod 26, …, c_n - k mod 26)

C	A	R	L	E	O	N	E
2	0	17	11	4	14	13	4

+

15

17	15	6	0	19	3	2	19
R	P	G	A	T	D	C	T

R	P	G	A	T	D	C	T
17	15	6	0	19	3	2	19

-

15

2	0	17	11	4	14	13	4
C	A	R	L	E	O	N	E

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

K = {0, 1, …, 25}   M = {A, B, …, Z} = {0, 1, …, 25}

Enc(m_1, …, m_n, k) = (m_1 + k mod 26, …, m_n + k mod 26)

Dec(c_1, …, c_n, k) = (c_1 - k mod 26, …, c_n - k mod 26)

C	A	R	L	E	O	N	E
2	0	17	11	4	14	13	4

\+ 15

17	15	6	0	19	3	2	19
R	P	G	A	T	D	C	T

Is it hard to break this cipher?

R	P	G	A	T	D	C	T
17	15	6	0	19	3	2	19

\- 15

2	0	17	11	4	14	13	4
C	A	R	L	E	O	N	E

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Let c be a ciphertext

- for every $k \in K$,
  check if Dec(c, k) is meaningful or not

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Let c be a ciphertext

- for every $k \in K$,
  check if Dec(c, k) is meaningful or not
- called brute force attack

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

F	D	U	O	H	R	Q	H
5	3	20	14	7	17	16	7

Let c be a ciphertext

- for every k ∈ K,
  check if Dec(c, k) is meaningful or not
- called brute force attack

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

F	D	U	O	H	R	Q	H
5	3	20	14	7	17	16	7
			−				
			1				
4	2	19	13	6	16	15	6
E	B	T	N	G	Q	P	G

Let c be a ciphertext

- for every $k \in K$,
  check if Dec(c, k) is meaningful or not
- called brute force attack

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

F	D	U	O	H	R	Q	H
5	3	20	14	7	17	16	7
			− 2				
3	1	18	12	5	15	14	5
D	B	S	M	F	P	O	F

Let c be a ciphertext

- for every k ∈ K,
  check if Dec(c, k) is meaningful or not
- called brute force attack

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

F	D	U	O	H	R	Q	H
5	3	20	14	7	17	16	7
			-				
			3				
2	0	17	11	4	14	13	4
C	A	R	L	E	O	N	E

Let c be a ciphertext

- for every k ∈ K,
  check if Dec(c, k) is meaningful or not
- called brute force attack

Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

F	D	U	O	H	R	Q	H
5	3	20	14	7	17	16	7

$-\ 3$

2	0	17	11	4	14	13	4
C	A	R	L	E	O	N	E

Let c be a ciphertext

- for every k ∈ K,
  check if Dec(c, k) is meaningful or not
- called brute force attack

at most 26 tries

Substitution Cipher
(Mono-alphabetic cipher)

A	B	C	D	E	F	G	H	I	J	K	L	M	N
E	S	J	T	U	O	F	A	Z	P	V	D	X	Q

O	P	Q	R	S	T	U	V	W	X	Y	Z
G	W	B	I	K	N	L	H	Y	C	M	R

Substitution Cipher
(Mono-alphabetic cipher)

A	B	C	D	E	F	G	H	I	J	K	L	M	N
E	S	J	T	U	O	F	A	Z	P	V	D	X	Q

O	P	Q	R	S	T	U	V	W	X	Y	Z
G	W	B	I	K	N	L	H	Y	C	M	R

K = a set of permutation of {0, 1, …, 25}
M = {A, B, …, Z} = {0, 1, …, 25}

$Enc(m_1, \ldots, m_n, \pi) = (\pi(m_1), \ldots, \pi(m_n))$

$Dec(c_1, \ldots, c_n, \pi) = (\pi^{-1}(c_1), \ldots, \pi^{-1}(c_n))$

Substitution Cipher
(Mono-alphabetic cipher)

A	B	C	D	E	F	G	H	I	J	K	L	M	N
E	S	J	T	U	O	F	A	Z	P	V	D	X	Q

O	P	Q	R	S	T	U	V	W	X	Y	Z
G	W	B	I	K	N	L	H	Y	C	M	R

CARLEONE

plaintext

K = a set of permutation of {0, 1, …, 25}
M = {A, B, …, Z} = {0, 1, …, 25}

$Enc(m_1, \ldots, m_n, \pi) = (\pi(m_1), \ldots, \pi(m_n))$

$Dec(c_1, \ldots, c_n, \pi) = (\pi^{-1}(c_1), \ldots, \pi^{-1}(c_n))$

Substitution Cipher
(Mono-alphabetic cipher)

A	B	C	D	E	F	G	H	I	J	K	L	M	N
E	S	J	T	U	O	F	A	Z	P	V	D	X	Q

O	P	Q	R	S	T	U	V	W	X	Y	Z
G	W	B	I	K	N	L	H	Y	C	M	R

CARLEONE → JEIDUGQU

plaintext ciphertext

K = a set of permutation of {0, 1, …, 25}
M = {A, B, …, Z} = {0, 1, …, 25}

$Enc(m_1, \ldots, m_n, \pi) = (\pi(m_1), \ldots, \pi(m_n))$

$Dec(c_1, \ldots, c_n, \pi) = (\pi^{-1}(c_1), \ldots, \pi^{-1}(c_n))$

Substitution Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
E	S	J	T	U	O	F	A	Z	P	V	D	X	Q

O	P	Q	R	S	T	U	V	W	X	Y	Z
G	W	B	I	K	N	L	H	Y	C	M	R

CARLEONE → JEIDUGQU

plaintext → ciphertext

- dominated the art of secret writing throughout the first millennium A.D.
- thought to be unbreakable by many back then

Substitution Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
E	S	J	T	U	O	F	A	Z	P	V	D	X	Q

O	P	Q	R	S	T	U	V	W	X	Y	Z
G	W	B	I	K	N	L	H	Y	C	M	R

CARLEONE → JEIDUGQU

plaintext ciphertext

How to break this cipher?

- dominated the art of secret writing throughout the first millennium A.D.
- thought to be unbreakable by many back then

Substitution Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
E	S	J	T	U	O	F	A	Z	P	V	D	X	Q

O	P	Q	R	S	T	U	V	W	X	Y	Z
G	W	B	I	K	N	L	H	Y	C	M	R

CARLEONE → JEIDUGQU

plaintext ciphertext

How to break this cipher?

the number of possible keys:

$26! \approx 4.03 \times 10^{26} \approx 2^{88}$

- dominated the art of secret writing throughout the first millennium A.D.
- thought to be unbreakable by many back then

Substitution Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
E	S	J	T	U	O	F	A	Z	P	V	D	X	Q

O	P	Q	R	S	T	U	V	W	X	Y	Z
G	W	B	I	K	N	L	H	Y	C	M	R

frequency analysis

- earliest known description of the technique is in a book by in a book by the ninth-century scientist Al Kindi for Arap text
- rediscovered or introduced in Europe in 1474 by Cicco Simonetta for Latin and Italian text

How to

the nu

26!

riting

m A.D.

many

back then

Substitution Cipher

- The frequency analysis of English alphabet

Letter	Percentage	Letter	Percentage
A	8.2	N	6.7
B	1.5	O	7.5
C	2.8	P	1.9
D	4.3	Q	0.1
E	12.7	R	6.0
F	2.2	S	6.3
G	2.0	T	9.1
H	6.1	U	2.8
I	7.0	V	1.0
J	0.2	W	2.4
K	0.8	X	0.2
L	4.0	Y	2.0
M	2.4	Z	0.1

- The most common bigrams :
  TH, HE, IN, EN, NT, RE, ER, AN, TI, ES

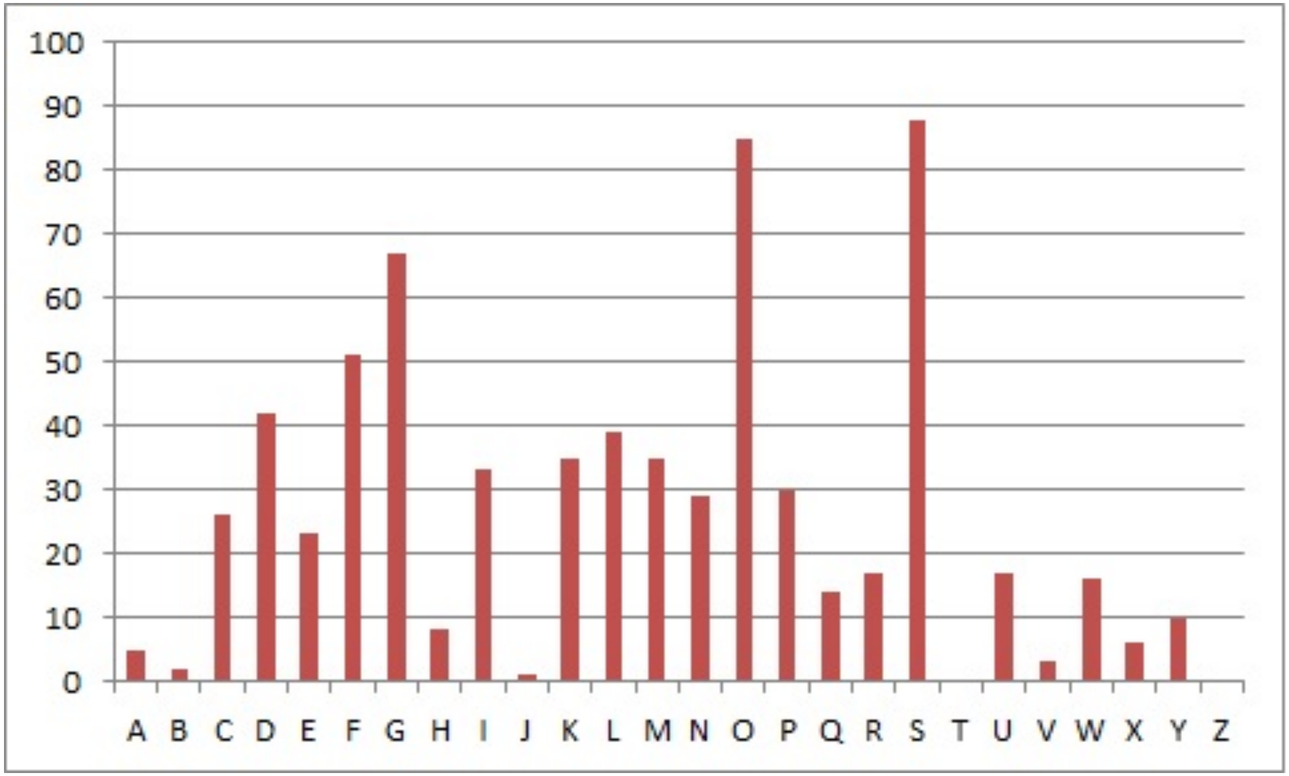
- The most common trigrams :
  THE, AND, THA, ENT, ING, ION, TIO, FOR, NDE, HAS

Substitution Cipher

« GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO', OIS FSXO EGLO GNNQKKPFR DSOOSK OIS 'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS 'OIPKU', MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS. »

Substitution Cipher

- the frequency analysis of the text :



- substitute S and O with E and T, respectively

Substitution Cipher

« GFe WMY tG LGDVe MF eFNKYHteU EeLLMRe, PC We BFGW PtL DMFRQMRe, PL tG CPFU M UPCCeKeFt HDMPFteXt GC tIe LMEe DMFRQMRe DGFR eFGQRI tG CPDD GFe LIeet GK LG, MFU tIeF We NGQFt tIe GNNQKKeFNeL GC eMNI DetteK. We NMDD tIe EGLt CKeJQeFtDY GNNQKKPFR DetteK tIe 'CPKLt', tIe FeXt EGLt GNNQKKPFR DetteK tIe 'LeNGFU' tIe CGDDGWPFR EGLt GNNQKKPFR DetteK tIe 'tIPKU', MFU LG GF, QFtPD We MNNGQFt CGK MDD tIe UPCCeKeFt DetteKL PF tIe HDMPFteXt LMEHDe. tIeF We DGGB Mt tIe NPHIeK teXt We WMFt tG LGDVe MFU We MDLG NDMLLPCY PtL LYEAGDL. We CPFU tIe EGLt GNNQKKPFR LYEAGD MFU NIMFRe Pt tG tIe CGKE GC tIe 'CPKLt' DetteK GC tIe HDMPFteXt LMEHDe, tIe FeXt EGLt NGEEGF LYEAGD PL NIMFReU tG tIe CGKE GC tIe 'LeNGFU' DetteK, MFU tIe CGDDGWPFR EGLt NGEEGF LYEAGD PL NIMFReU tG tIe CGKE GC tIe 'tIPKU' DetteK, MFU LG GF, QFtPD We MNNGQFt CGK MDD LYEAGDL GC tIe NKYHtGRKME We WMFt tG LGDVe. »

Substitution Cipher

- The most common trigram in the text is TLE, which can be THE.

So, substitute L with H.

Substitution Cipher

- The most common trigram in the text is TLE, which can be THE.

So, substitute L with H.

- The next common in the text is G which could be A, I, or O

Substitution Cipher

- The most common trigram in the text is TLE, which can be THE.

So, substitute L with H.

- The next common in the text is G which could be A, I, or O

The third word is tG - only 'to' makes sense -

Substitution Cipher

« oFe WMY to LoDVe MF eFNKYHteU EeLLMRe, PC We BFoW PtL DMFRQMRe, PL to CPFU M UPCCeKeFt HDMPFteXt oC the LMEe DMFRQMRe DoFR eFoQRh to CPDD oFe Lheet oK Lo, MFU theF We NoQFt the oNNQKKeFNeL oC eMNh DetteK. We NMDD the EoLt CKeJQeFtDY oNNQKKPFR DetteK the 'CPKLt', the FeXt EoLt oNNQKKPFR DetteK the 'LeNoFU' the CoDDoWPFR EoLt oNNQKKPFR DetteK the 'thPKU', MFU Lo oF, QFtPD We MNNoQFt CoK MDD the UPCCeKeFt DetteKL PF the HDMPFteXt LMEHDe. theF We DooB Mt the NPHheK teXt We WMFt to LoDVe MFU We MDLo NDMLLPCY PtL LYEAoDL. We CPFU the EoLt oNNQKKPFR LYEAoD MFU NhMFRe Pt to the CoKE oC the 'CPKLt' DetteK oC the HDMPFteXt LMEHDe, the FeXt EoLt NoEEoF LYEAoD PL NhMFReU to the CoKE oC the 'LeNoFU' DetteK, MFU the CoDDoWPFR EoLt NoEEoF LYEAoD PL NhMFReU to the CoKE oC the 'thPKU' DetteK, MFU Lo oF, QFtPD We MNNoQFt CoK MDD LYEAoDL oC the NKYHtoRKME We WMFt to LoDVe. »

Substitution Cipher

« one way to solve an encrypted message, if we know its language, is to find a different plaintext of the same language long enough to fill one sheet or so, and then we count the occurrences of each letter. we call the most frequently occurring letter the 'first', the next most occurring letter the 'second' the following most occurring letter the 'third', and so on, until we account for all the different letters in the plaintext sample. then we look at the cipher text we want to solve and we also classify its symbols. we find the most occurring symbol and change it to the form of the 'first' letter of the plaintext sample, the next most common symbol is changed to the form of the 'second' letter, and the following most common symbol is changed to the form of the 'third' letter, and so on, until we account for all symbols of the cryptogram we want to solve. »

Poly-alphabetic Cipher

- main weaknesses of mono-alphabetic substitution ciphers
  - each letter in the ciphertext corresponds to only one letter in the plaintext

Poly-alphabetic Cipher

- main weaknesses of mono-alphabetic substitution ciphers
  - each letter in the ciphertext corresponds to only one letter in the plaintext
- idea for a stronger cipher (1460 by Alberti)
  - use more than one cipher alphabet, and switch between them when encrypting different letters

Poly-alphabetic Cipher

- main weaknesses of mono-alphabetic substitution ciphers
  - each letter in the ciphertext corresponds to only one letter in the plaintext
- idea for a stronger cipher (1460 by Alberti)
  - use more than one cipher alphabet, and switch between them when encrypting different letters
- Giovani Battista Bellaso published it in 1553

Poly-alphabetic Cipher

- main weaknesses of mono-alphabetic substitution ciphers
  - each letter in the ciphertext corresponds to only one letter in the plaintext
- idea for a stronger cipher (1460 by Alberti)
  - use more than one cipher alphabet, and switch between them when encrypting different letters
- Giovani Battista Bellaso published it in 1553
- developed into a practical cipher by Blaise de Vigenère and published in 1586

Vigenere Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
O	P	Q	R	S	T	U	V	W	X	Y	Z		
14	15	16	17	18	19	20	21	22	23	24	25		

K = a set of characters $\{k_1, \dots, k_p\}$
$M = \{A, B, \dots, Z\} = \{0, 1, \dots, 25\}$

$$Enc(m_1, \dots, m_n, k) = (m_1 + k_1 \bmod 26, \dots, m_p + k_p \bmod 26,$$
$$m_{(p+1)} + k_1 \bmod 26, \dots, m_{2p} + k_p \bmod 26,$$
$$\dots)$$

$$Dec(c_1, \dots, c_n, k) = (c_1 - k_1 \bmod 26, \dots, c_p - k_p \bmod 26,$$
$$c_{(p+1)} - k_1 \bmod 26, \dots, c_{2p} - k_p \bmod 26,$$
$$\dots)$$

Vigenere Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

key : ARC

C	A	R	L	E	O	N	E
2	0	17	11	4	14	13	4

Vigenere Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

key : ARC

C	A	R	L	E	O	N	E
2	0	17	11	4	14	13	4
			+				
A	R	C	A	R	C	A	R
0	17	2	0	17	2	0	17

Vigenere Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

key : ARC

C	A	R	L	E	O	N	E
2	0	17	11	4	14	13	4
			+				
A	R	C	A	R	C	A	R
0	17	2	0	17	2	0	17
2	17	19	11	21	16	13	21
C	R	T	L	V	Q	N	V

Vigenere Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

key : ARC

C	A	R	L	E	O	N	E
2	0	17	11	4	14	13	4
			+				
A	R	C	A	R	C	A	R
0	17	2	0	17	2	0	17
2	17	19	11	21	16	13	21
C	R	T	L	V	Q	N	V

- one letter in the ciphertext corresponds to multiple letters in the plaintext
- makes the use of frequency analysis more difficult

Vigenere Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

key : ARC

C	A	R	L	E	O	N	E
2	0	17	11	4	14	13	4
			+				
A	R	C	A	R	C	A	R
0	17	2	0	17	2	0	17
2	17	19	11	21	16	13	21
C	R	T	L	V	Q	N	V

How to break Vigenere cipher

- find the length of the key

Vigenere Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

key : ARC

C	A	R	L	E	O	N	E
2	0	17	11	4	14	13	4
				+			
A	R	C	A	R	C	A	R
0	17	2	0	17	2	0	17
2	17	19	11	21	16	13	21
C	R	T	L	V	Q	N	V

How to break Vigenere cipher

- find the length of the key
  - Kasisky test (1863)
  - the index of coincidence by Friedman (1920)

Vigenere Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

key : ARC

C	A	R	L	E	O	N	E
2	0	17	11	4	14	13	4
			+				
A	R	C	A	R	C	A	R
0	17	2	0	17	2	0	17
2	17	19	11	21	16	13	21
C	R	T	L	V	Q	N	V

How to break Vigenere cipher

- find the length of the key
  - Kasisky test (1863)
  - the index of coincidence by Friedman (1920)
- divide the messag into that many shift ciphers
- use frequency analysis to solve it

Vigenere Cipher
(Kasinsky Test)

Plaintext T H E S U N A N D T H E M A N I N T H E M O O N

Vigenere Cipher (Kasinsky Test)

Plaintext	T H E S U N A N D T H E M A N I N T H E M O O N
Key	K I N G K I N G K I N G K I N G K I N G K I N G

Vigenere Cipher (Kasinsky Test)

Plaintext	T	H	E	S	U	N	A	N	D	T	H	E	M	A	N	I	N	T	H	E	M	O	O	N
Key	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G
Ciphertext	D	P	R	Y	E	V	N	T	N	B	U	K	W	I	A	O	X	B	U	K	W	W	B	T

Vigenere Cipher (Kasinsky Test)

Plaintext	T H E S U N A N D T H E M A N I N T H E M O O N
Key	K I N G K I N G K I N G K I N G K I N G K I N G
Ciphertext	D P R Y E V N T N B U K W I A O X B U K W W B T

Vigenere Cipher (Kasinsky Test)

Plaintext	T H E S U N A N D **T H E** M A N I N **T H E** M O O N
Key	K I N G K I N G K **I N G** K I N G K **I N G** K I N G
Ciphertext	D P R Y E V N T N **B U K** W I A O X **B U K** W W B T

distance = 8

Vigenere Cipher (Kasinsky Test)

Plaintext	T	H	E	S	U	N	A	N	D	T	H	E	M	A	N	I	N	T	H	E	M	O	O	N
Key	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G
Ciphertext	D	P	R	Y	E	V	N	T	N	B	U	K	W	I	A	O	X	B	U	K	W	W	B	T

distance = 8

- distance between duplicate n-grams in ciphertext is multiple of cipher period (key length)

Vigenere Cipher (Kasinsky Test)

Plaintext	T	H	E	S	U	N	A	N	D	T	H	E	M	A	N	I	N	T	H	E	M	O	O	N
Key	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G
Ciphertext	D	P	R	Y	E	V	N	T	N	B	U	K	W	I	A	O	X	B	U	K	W	W	B	T

distance = 8

- distance between duplicate n-grams in ciphertext is multiple of cipher period (key length)
- search for pairs of identical segments of length at least 3

Vigenere Cipher (Kasinsky Test)

Plaintext	T	H	E	S	U	N	A	N	D	T	H	E	M	A	N	I	N	T	H	E	M	O	O	N
Key	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G
Ciphertext	D	P	R	Y	E	V	N	T	N	B	U	K	W	I	A	O	X	B	U	K	W	W	B	T

distance = 8

- distance between duplicate n-grams in ciphertext is multiple of cipher period (key length)
- search for pairs of identical segments of length at least 3
- period p divides gcm(d_1, d_2, …)