

Cryptography Fundamentals

Traditional ciphers.

Frequency Analysis.

Operators and GCD.

Encoding.

Big Integers.

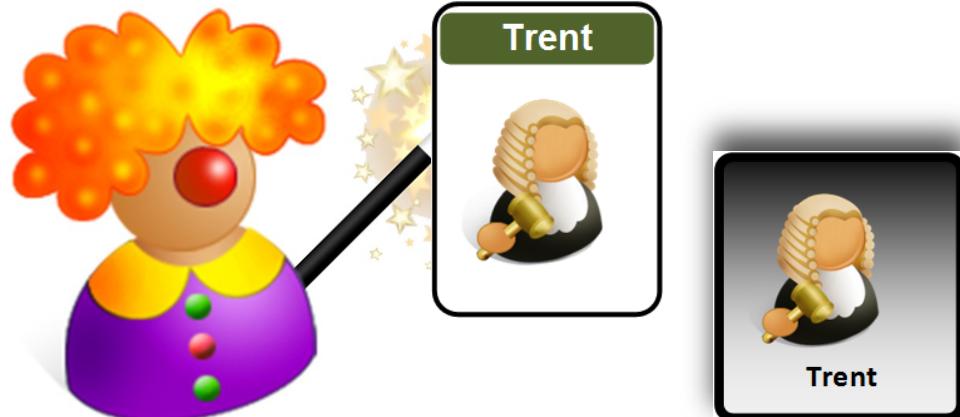
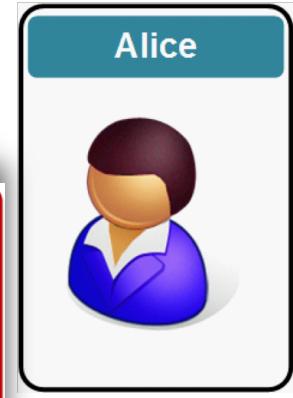
Random Numbers.

Key-based Encryption.

Prof Bill Buchanan

<http://asecuritysite.com/encryption>

Encryption



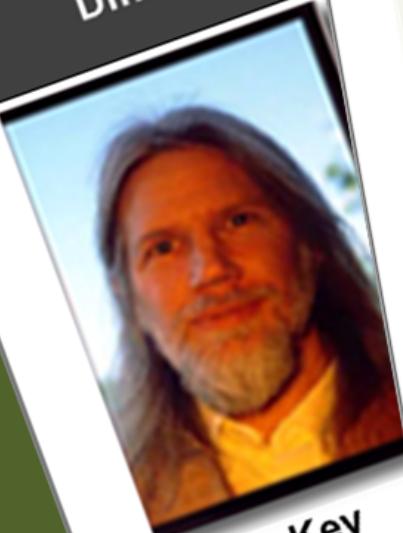
- Encryption works great, until it doesn't.
- Encryption works great, as long as no one makes a mistake.
- Encryption works great, unless something goes wrong.
- Encryption works great, as long as everything works right.

Bruce Schneier



Twofish,
Blowfish

Whitfield
Diffie



Key
interchange

Rivest, Shamir
& Alderman



Public-k
encryp'

Ron
Rivest



Hashing

AES
Modern private
key encryption

Phil
Zimmerman

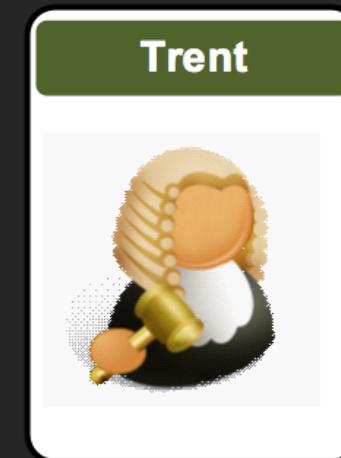
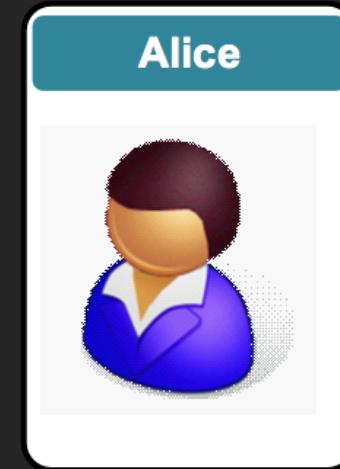


PGP
Encryption

Advanced Crypto

1. Ciphers and Fundamentals

Ciphers.



<http://asecuritysite.com/crypto>

Author: Prof Bill Buchanan



Quilt codes



Flying geese



Sailboat



Smoke signals

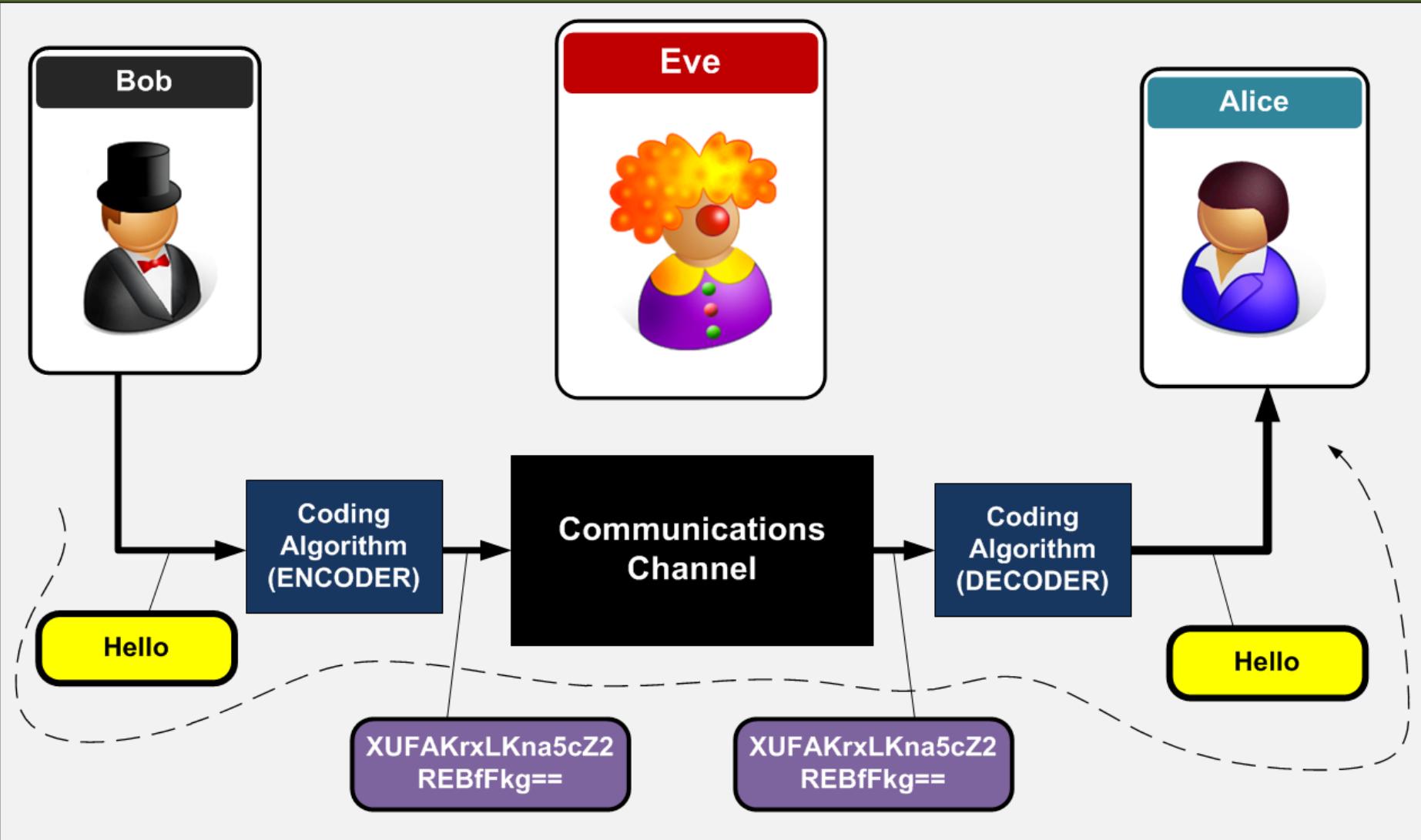


Microfiche

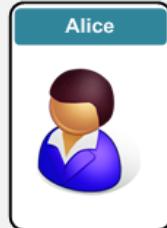
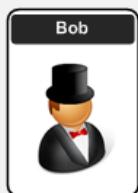


Navajo Code Talkers

Early Code



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	(- - - - - -)				



Plaintext
Morse:

h e l l o e v e r y o n e
.... . -... --- . -. -.- -.- - -



Early Code

Morse Code

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y/Z

Polybius (Greek historian,
~200BC)



HELLO
23 15 32 32 35



A	B	C
D	E	F
H	I	

J.	K.	L
M.	N.	O
P.	Q.	R

~~S
T
U
V~~

~~W
X
Y
Z~~



Headstone of James Leeson (1792)



THE FREEMASON CIPHER		
A	B	C
D	E	F
G	H	I
J	K	L
M		
N	O	P
Q	R	S
T	U	V
K = >	T = □	
N = □	E = □	
I = □	M = ▲	
G = □	P = ▽	
H = □	L = <	
T = □	A = □	
S = □	R = □	



	A	D	F	G	V	X
A	8	p	3	d	1	n
D	1	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q



Invented by Fritz
Nebel, in WW1



FD VG VV FD FG DV DA AG XF





Charles
Wheatstone



Lord
Playfair

Code: **NAPIERUN**

Write out the 5x5 matrix,
and do not repeat
characters (get rid of Q
and J):

N	A	P	I	E
R	U	NiaB	C	
D	e	F	G	Hi K
L	Mn	OprS	Tu	
V	W	X	Y	Z

AT

TA

CK

N	A	P	I	E
R	U	NiaB	C	
D	e	F	G	Hi K
L	Mn	OprS	Tu	
V	W	X	Y	Z

N	A	P	I	E
R	U	NiaB	C	
D	e	F	G	Hi K
L	Mn	OprS	Tu	
V	W	X	Y	Z

N	A	P	I	E
R	U	NiaB	C	
D	e	F	G	Hi K
L	Mn	OprS	Tu	
V	W	X	Y	Z

ME

EM

KT

Rules:

- If the are in different columns, takes from the rectangle defined between them and pick off the opposite ends.
- If the are in the same column, select the letter one below (and wrap-round if necessary).

Caesar



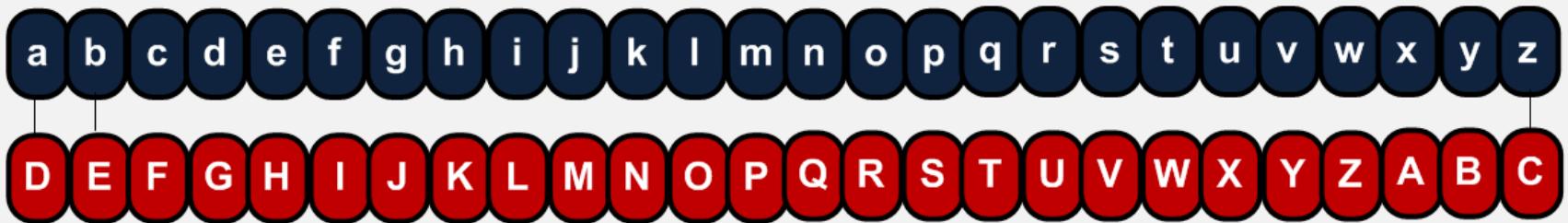
Mark Antony



Cleopatra



Plaintext



Ciphertext

K H O O R



Early Code

Caesar Cipher

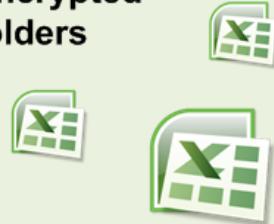


2011, **Rajib Karim**, - a greater threat than Bin Laden - a Software Engineer for British Airways, had a massive plot to blow up an in-air transatlantic jet.

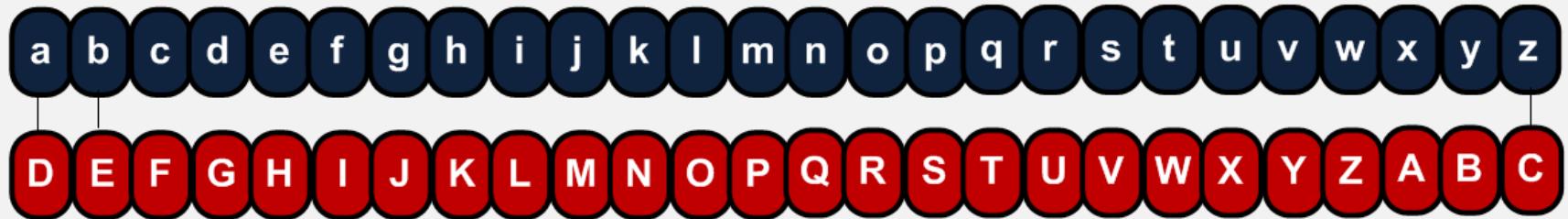
Used Excel documents with Caeser codes, instead of PGP (because 'kaffirs' - non-believers – knew about PGP)

Protected by
a password

Encrypted
folders



Plaintext



Ciphertext

K H O O R



Early Code

Caesar Cipher

Caesar



Mark Antony



Cleopatra



Plaintext

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

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

Ciphertext

L Q N Z D O O



Caesar



Mark Antony



Cleopatra



Plaintext

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

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

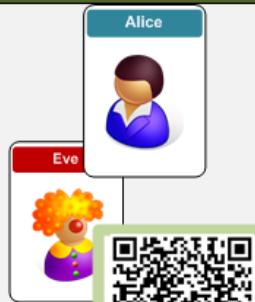
Ciphertext

L Q N Z D O O

4×10^{26} code
mappings

$$26! = 26 \times 25 \times 24 \times \dots \times 2 \times 1 = 403,291,461,126,605,635,584,000,000 \text{ codes}$$





ONR ECRYAPFJ FDAO PFOXADRT NPM TGOG UGD LR
 RDUCIEORT JP ONGO AO UGDDPO LR YARMRT LI GDIPDF
 AO MGJ DPO ADORDTRT QCPK. MAON ECAYGOR-SRI
 RDUCIEOAPD, LPL GDT GXAUR FJR ONR JGKR JRUCRO SRI OP
 RDUCIEO GDT TRUCIEO ONR KRJJGZR. ONRD, FJADZ G SRI
 ADORCUNGDR KRONPT JFUN GJ TAQQAR-NRXXKGD, LPL GDT
 GXAUR UGD ZDRDCGOR ONR JGKR JRUCRO SRI, RYRD AQ RYR
 AJ XAJORDADZ OP ONRAC UPKKFDAUGOAPDJ. MAON EFLXAU-
 SRI RDUCIEOAPD, LPL GDT GXAUR TP DPO NGYR ONR JGKR
 ECPLXRK, GJ GXAUR UGD GTYRCOAJR NRC EFLXAU SRI JP
 ONGO LPL UGD FJR AO OP RDUCIEO UPKKFDAUGOAPDJ OP NRC.
 ONR PDXI SRI ONGO UGD TRUCIEO ONR UPKKFDAUGOAPDJ AJ
 GXAUR'J ECAYGOR SRI (MNAUN, NPERQFXI, RYR UGDDPO ZRO
 NPXT PQQ). MR DPM, ONPFZN, NGYR QPFC QFCONRC
 ECPLXRKJ:- NPM TP MR SDPM ONGO AO MGJ CRGXXI LPL MNP
 JRDO ONR TGOG, GJ GDIPDR UGD ZRO GXAUR'J EFLXAU SRI,
 GDT ONFJ ECRORDT OP LR LPL? - NPM UGD MR ORXX ONGO
 ONR KRJJGZR NGJ DPO LRRD OGKERCRT MAON? - NPM TPRJ
 LPL TAJOCALFOR NAJ EFLXAU SRI OP GXAUR, MAONPFO
 NGYADZ OP EPJO AO PDOP G MRL JAOR PC QPC LPL OP LR PD-
 XADR MNRD GXAUR CRGTJ ONR KRJJGZR? - MNP UGD MR
 CRGXXI OCFJO OP ECPERCXI GFONRDOAUGOR LPL? PLYAPFJXI
 MR UGD'O OCFJO LPL OP GFONRDOAUGOR ONGO NR CRGXXI AJ
 LPL. ONRJR WFRJOAPDJ MAXX LR GDJMRCRT AD ONAJ FDAO, GJ
 MR MAXX XPPS GO ONR FJGZR PQ NGJNADZ OP QADZRC-ECADO
 TGOG, GDT ONRD NPM LPL'J ECAYGOR SRI UGD LR FJRT OP
 GFONRDOAUGOR NAKJRXQ. QADGXXI, AO MAXX XPPS GO ONR
 MGI ONGO G EFLXAU SRI UGD LR TAJOCALFORT, FJADZ
 TAZAOGX URCOAQ AUGORJ, MNAUN UGD UGCCI RDUCIEOAPD
 SRI. ONAJ UNGEORC MAXX JNPM ONR AKEPCOGDUR PQ
 GFONRDOAUGOAPD GDT GJJFCGDUR, GXPDZ MAON
 UPDQATRDOAGXAOI (QAZFCR 4.1), GDT ONR FJGZR PQ
 LAPKROCAUJ.

Letters (%)	Digrams (%)	Trigrams (%)	Words (%)
E 13.05	TH 3.16	THE 4.72	THE 6.42
T 9.02	IN 1.54	ING 1.42	OF 4.02
O 8.21	ER 1.33	AND 1.13	AND 3.15
A 7.81	RE 1.30	ION 1.00	TO 2.36
N 7.28	AN 1.08	ENT 0.98	A 2.09
I 6.77	HE 1.08	FOR 0.76	IN 1.77
R 6.64	AR 1.02	TIO 0.75	THAT 1.25
S 6.46	EN 1.02	ERE 0.69	IS 1.03
H 5.85	TI 1.02	HER 0.68	I 0.94
D 4.11	TE 0.98	ATE 0.66	IT 0.93
L 3.60	AT 0.88	VER 0.63	FOR 0.77
C 2.93	ON 0.84	TER 0.62	AS 0.76
F 2.88	HA 0.84	THA 0.62	WITH 0.76
U 2.77	OU 0.72	ATI 0.59	WAS 0.72
M 2.62	IT 0.71	HAT 0.55	HIS 0.71
P 2.15	ES 0.69	ERS 0.54	HE 0.71
Y 1.51	ST 0.68	HIS 0.52	BE 0.63
W 1.49	OR 0.68	RES 0.50	NOT 0.61
G 1.39	NT 0.67	ILL 0.47	BY 0.57
B 1.28	HI 0.66	ARE 0.46	BUT 0.56
V 1.00	EA 0.64	CON 0.45	HAVE 0.55
K 0.42	VE 0.64	NCE 0.43	YOU 0.55
X 0.30	CO 0.59	ALL 0.44	WHICH 0.53
J 0.23	DE 0.55	EVE 0.44	ARE 0.50
Q 0.14	RA 0.55	ITH 0.44	ON 0.47
Z 0.09	RO 0.55	TED 0.44	OR 0.45



Bob	Plaintext:	abcdefghijklmnopqrstuvwxyz	Gen another
	Scrambled code:	GLUTRQZNABSXKDPEWCJOFYMVIIH	
Message:	<p>The previous unit outlined how data can be encrypted so that it cannot be viewed by anyone that it was not intended from. With private-key encryption, Bob and Alice use the same secret key to encrypt and decrypt the message. Then, using a key interchange method such as Diffie-Hellman, Bob and Alice can generate the same secret key, even if Eve is listening to their communications. With public-key</p>		
Encoded:	<pre>ONR ECRYAPFJ FDAO PFOXADRT NPM TGOG UGD LR RDUCIEORT JP ONGO AO UGDDPO LR YARMRT LI GDIPDR ONGO AO MGJ DPO ADORDTRT QCPK. MAON ECAYGOR-SRI RDUCIEOAPD, LPL GDT GXAUR FJR ONR JGKR JRUCRO SRI OP RDUCIEO GDT TRUCIEO ONR KRJJGZR. ONRD, FJADZ G SRI ADORCUNGDRZ KRONPT JFUN GJ TAAQAR-NRXXKGD, LPL GDT GXAUR UGD ZDRRCGOR ONR JGKR JRUCRO SRI, RYRD AQ RYR AJ XAJORDADZ OP ONRAC UPKKFDAUGOAPDJ. MAON EFLXAU-SRI</pre>		
		Convert	

Frequency Analysis of Text

This table shows the occurrences of the letters in the text (ignoring the case of the letters):

a	b	c	d	e	f	g	h	i	j	k	l	m
95 [7.1%]	0 [0.0%]	51 [3.8%]	90 [6.8%]	28 [2.1%]	38 [2.9%]	105 [7.9%]	0 [0.0%]	35 [2.6%]	66 [5.0%]	21 [1.6%]	45 [3.4%]	34 [2.6%]
n	o	p	q	r	s	t	u	v	w	x	y	z
72 [5.4%]	138 [10.4%]	90 [6.8%]	19 [1.4%]	159 [11.9%]	16 [1.2%]	35 [2.6%]	59 [4.4%]	0 [0.0%]	1 [0.1%]	50 [3.8%]	13 [1.0%]	19 [1.4%]

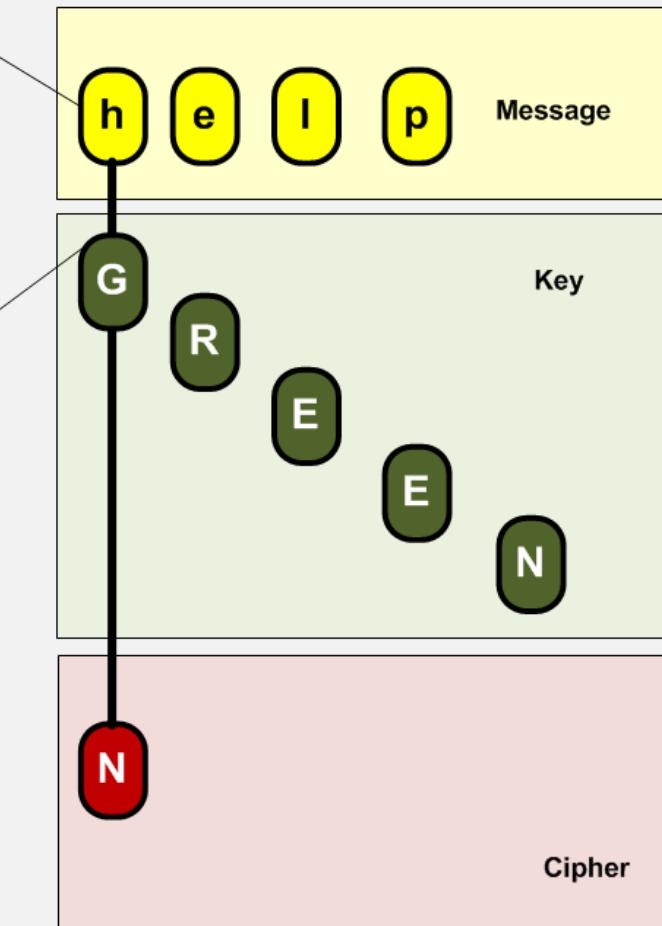
Mapping to normal

This table shows how the text matches a normal probability to text (where 'E' has the highest level of occurrence and 'Z' has the least). The grey rows show what would be expected for the order, and the red one shows what your text gives for the order:

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

UPDQATRDOAGXAOI (QAZFCR 4.1), GDT ONR FJGZR PQ LAPKROCAUJ.	z 0.09	RO 0.55	TED 0.44	OR 0.45
--	--------	---------	----------	---------

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

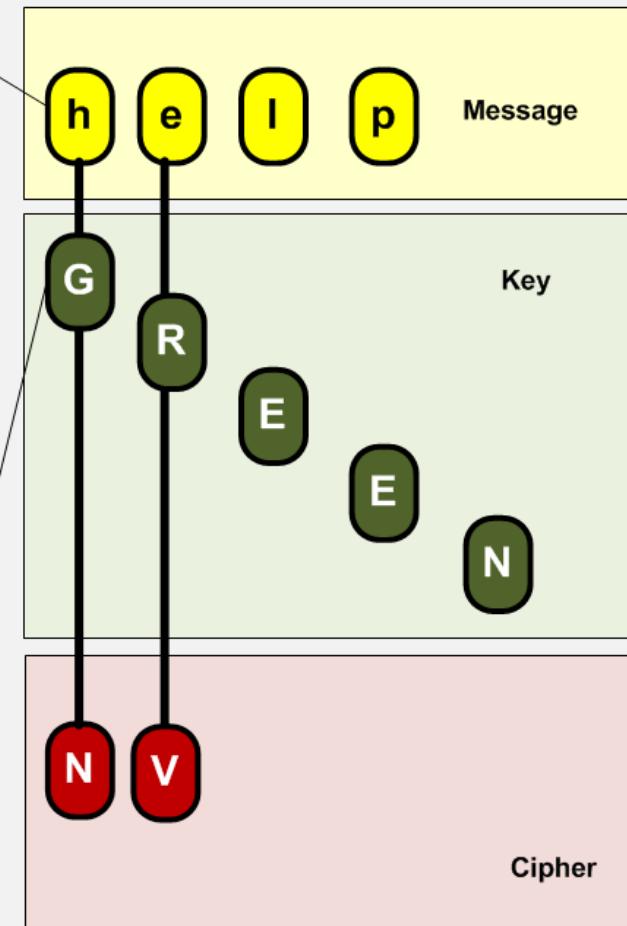


Vigenère cipher

- In 1553, invented by Giovan Battista Bellaso.
 - In 1900s, attributed to Blaise de Vigenère.



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

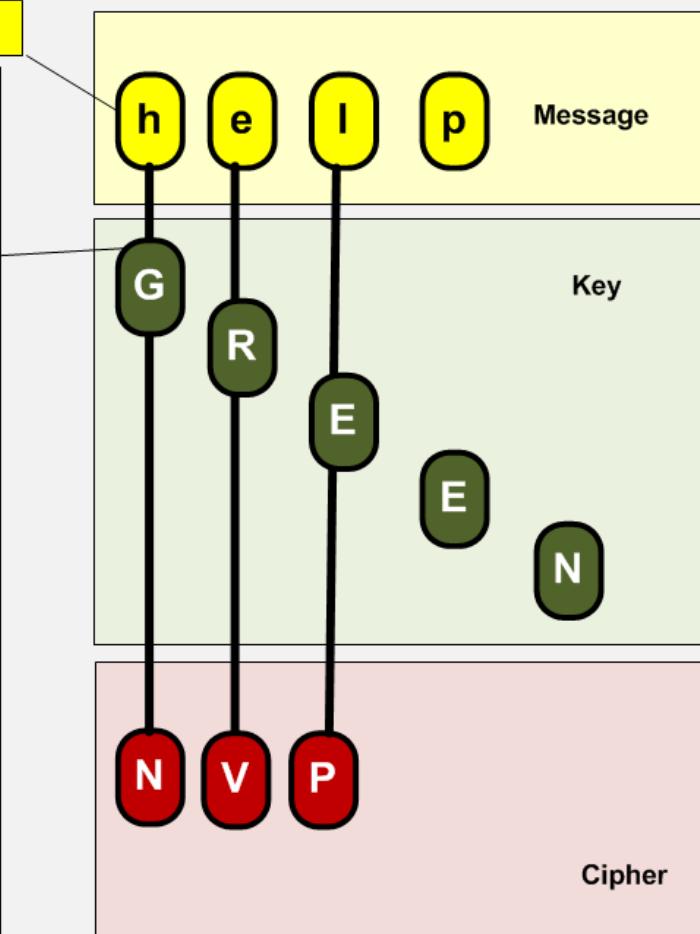


Vigenère cipher

- In 1553, invented by Giovan Battista Bellaso.
- In 1900s, attributed to Blaise de Vigenère.



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

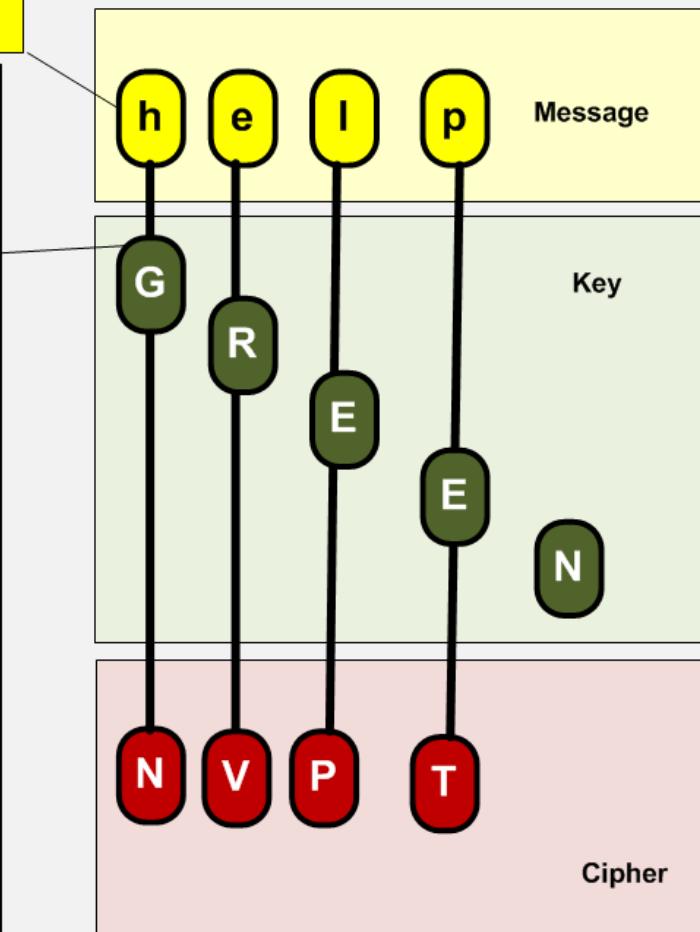


Vigenère cipher

- In 1553, invented by Giovan Battista Bellaso.
- In 1900s, attributed to Blaise de Vigenère.



	abcdefghijklmnopqrstuvwxyz	abcdefghijklmnopqrstuvwxyz
A	ABCDEFGHIJKLMNO	PQRSTUVWXYZ
B	BCDEFGHIJKLMNO	PQRSTUVWXYZA
C	CDEFGHIJKLMNO	PQRSTUVWXYZAB
D	DEFGHIJKLMNO	PQRSTUVWXYZABC
E	FGHIJKLMNO	PQRSTUVWXYZABCD
F	GHIJKLMNO	PQRSTUVWXYZABCDE
G	HJKLMNO	PQRSTUVWXYZABCDEF
H	IJKLMNO	PQRSTUVWXYZABCDEF
I	JJKLMNO	PQRSTUVWXYZABCDEF
J	KJKLMNO	PQRSTUVWXYZABCDEF
K	LJKLMNO	PQRSTUVWXYZABCDEF
L	MJKLMNO	PQRSTUVWXYZABCDEF
M	NJKLMNO	PQRSTUVWXYZABCDEF
N	OJKLMNO	PQRSTUVWXYZABCDEF
O	OPJKLMNO	PQRSTUVWXYZABCDEF
P	OPQRSTUVWXYZ	AJKLMNOPQRSTUVWXYZ
Q	QRSTUVWXYZ	BJKLMNOPQRSTUVWXYZ
R	QRSTUVWXYZ	CJKLMNOPQRSTUVWXYZ
S	QRSTUVWXYZ	DJKLMNOPQRSTUVWXYZ
T	QRSTUVWXYZ	EJKLMNOPQRSTUVWXYZ
U	QRSTUVWXYZ	FJKLMNOPQRSTUVWXYZ
V	QRSTUVWXYZ	GJKLMNOPQRSTUVWXYZ
W	QRSTUVWXYZ	HJKLMNOPQRSTUVWXYZ
X	QRSTUVWXYZ	IJKLMNOPQRSTUVWXYZ
Y	QRSTUVWXYZ	JJKLMNOPQRSTUVWXYZ
Z	QRSTUVWXYZ	KJKLMNOPQRSTUVWXYZ



Vigenère cipher

- In 1553, invented by Giovan Battista Bellaso.
- In 1900s, attributed to Blaise de Vigenère.



Vigenère Calculator

[\[Back\]](#) This page defines a Vigenère Calculator:

Enter Word:

[help](#)

Enter Key:

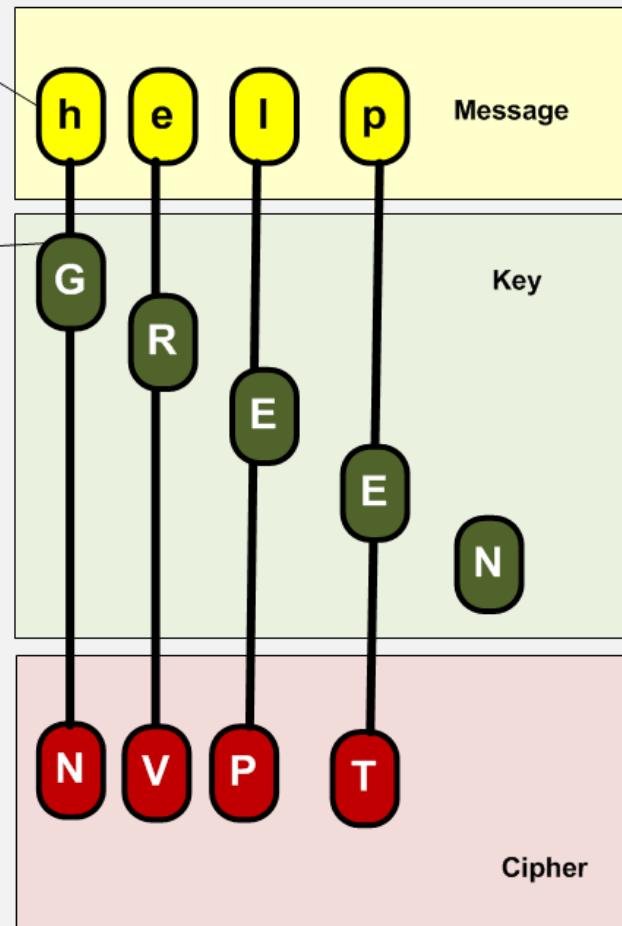
[green](#)

[Analyse](#)

Code: [nvpt](#)

Decode (just to check): [help](#)

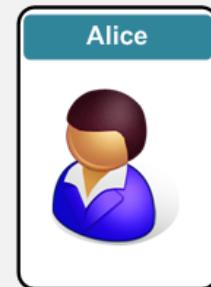
M	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R	R S T U V W X Y Z A B C D E F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



Vigenère cipher

- In 1553, invented by Giovan Battista Bellaso.
- In 1900s, attributed to Blaise de Vigenère.





Bob generates a random code book

```
gvlpj iqqxe wmrnn bxwhi mqmqt  
zmuvz cpmaq rlvtn kkfij jowet  
xqfuh pjvvk vwuyc gaqvv qbdty  
bldgj kqpcc lkrtb hpajr opggd  
jybjc wnlwf egplz fgsvr wjwun  
batbj mexda mogag xyunw baojm  
hwloh zbhvb vtjns ajmkn qzrpt  
xpjym amkpb ptiva khzl eohuv  
rovvv ievvk ksjja jjuld hbqkd  
josep iiociu miout kxmlq rybzb
```

Bob sends Alice
the code book

```
gvlpj iqqxe wmrnn bxwhi mqmqt  
zmuvz cpmaq rlvtn kkfij jowet  
xqfuh pjvvk vwuyc gaqvv qbdty  
bldgj kqpcc lkrtb hpajr opggd  
jybjc wnlwf egplz fgsvr wjwun  
batbj mexda mogag xyunw baojm  
hwloh zbhvb vtjns ajmkn qzrpt  
xpjym amkpb ptiva khzl eohuv  
rovvv ievvk ksjja jjuld hbqkd  
josep iiociu miout kxmlq rybzb
```

Bob uses a random sequence for his code:
[198][197][208][170][131][161][227][190]

To give: **uhvqetsk**

Using Vigenère gives
Message: **shetland**
Key: **uhvqetsk**
Ciper: **mozjptfn**



Bob sends Alice
the key

Bob sends cipher:
mozjptfn

Using the pad, key and cipher,
Alice can now decrypt:

Message: **shetland**



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
07	11	17	10	25	08	44	19	02	18	41	42	40	00	16	01	15	04	06	05	13	22	45	12	55	47
31	64	33	27	26	09	83	20	03		81	52	43	30	62		24	34	23	14		46		93		
50		49	51	28			21	29		86		80	61			39	56	35	36						
63			76	32			54	53		95		88	65			58	57	37							
66				48			70	68				89	91			71	59	38							
77					67		87	73				94				00	90	60							
84					69							96					74					78			92
					72																				
					75																				
					79																				
					82																				
					85																				

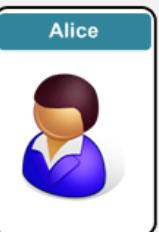


Plaintext

h e l l o e v e r y o n e

Ciphertext:

19 25 42 81 16 26 22 28 04 55 30 00 32



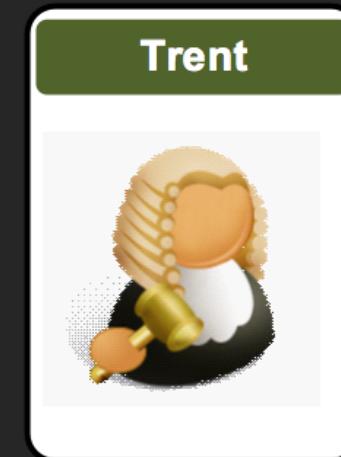
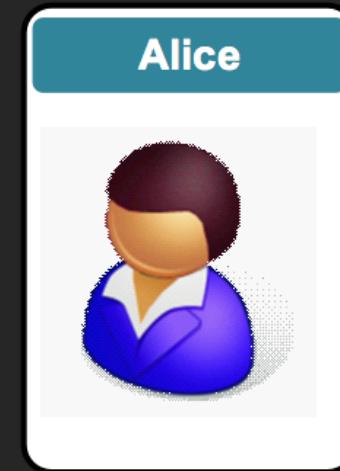
Advanced Crypto

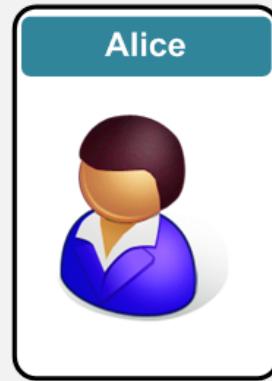
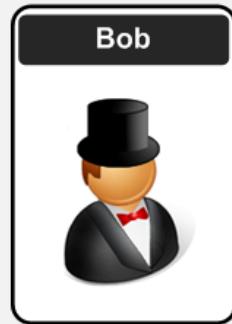
1. Ciphers and Fundamentals

Encoding Methods

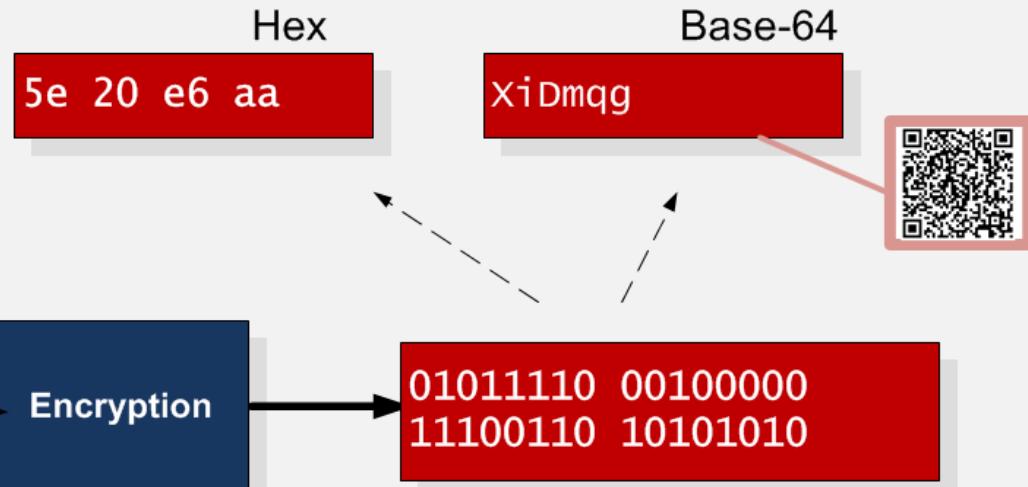
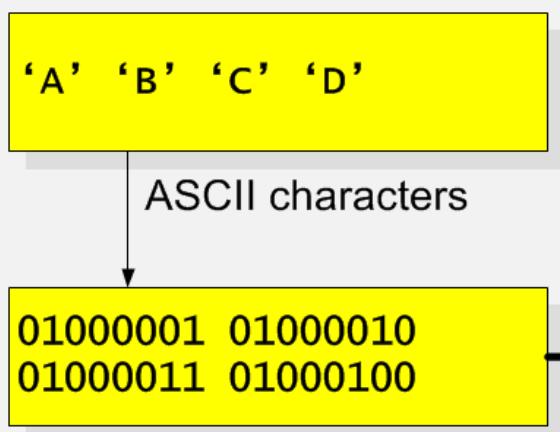
<http://asecuritysite.com/crypto>

Author: Prof Bill Buchanan





Binary values are difficult to view/edit, thus encrypted values are typically converted to hex or Base-64.





With hexadecimal, the bit stream is split into groups of four, and converted into hex values (0-9,A-F)

0101 1110 0010 0000 1110 0110 1010 1010

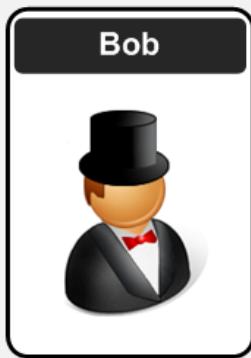
Bit stream

5 e 2 0 e 6 a a

Hex

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





01100110 01110010 01100101 01100100

011001 100111 001001 100101 011001 00

Bit stream

Z n J l Z A = =

Base-64

Encoding

Base-64

With Base-64, the bits are split into groups of six, and then converted. Base-64 is used extensively on the Internet (such as in email).

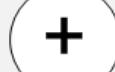
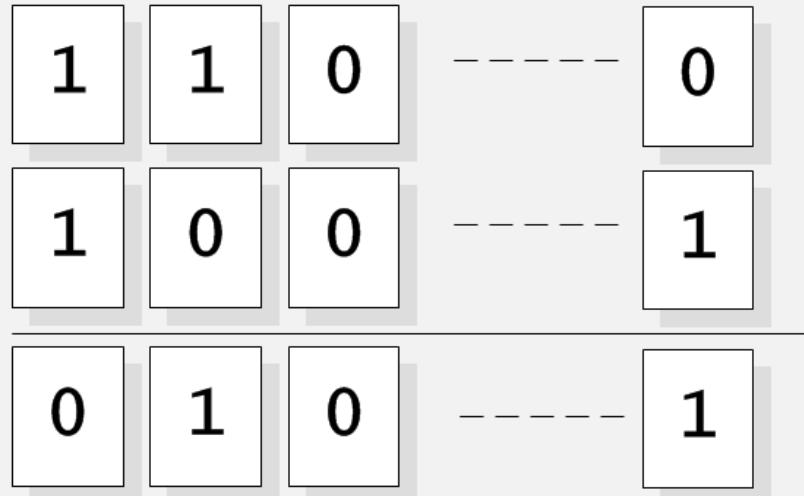
Val	Enc	Val	Enc	Val	Enc	Val	Enc
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/





The two main operators used in encryption are Ex-OR and ROR/ROL

The two main operators used in encryption are Ex-OR and ROR/ROL, as they are fast, and preserve info.



Exclusive-OR
operation

0 1 1 0 0 0 0 0

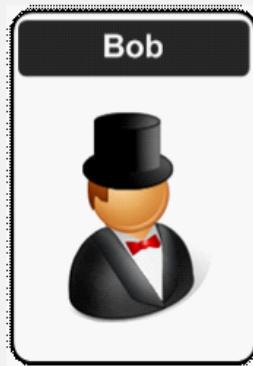
Rotate left (ROL) 2 bits

1 0 0 0 0 0 0 1

Rotate left (ROL)

Rotate right (ROR)





The modulus is the remainder of a divide

The Mod operator is used extensively in cryptography

143 mod 5

28 rem 3

3

87 mod 9?



**UTF-16****ASCII**

Non Printable:
New line (0x13)
Tab (0x07)
Backspace (0x08)

Printable:
Space (0x20)

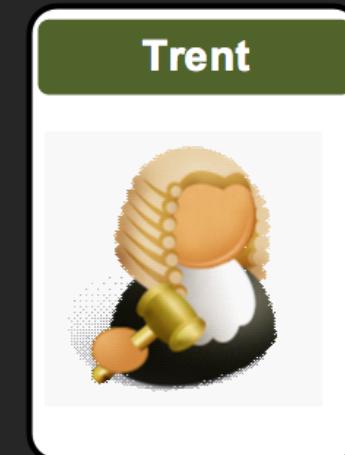
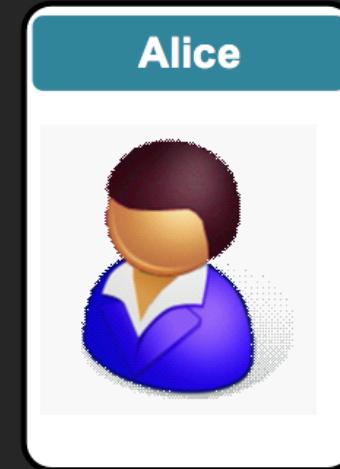
A	65	00000000001000001	41	101	A
B	66	00000000001000010	42	102	B
C	67	00000000001000011	43	103	C
D	68	00000000001000100	44	104	D
E	69	00000000001000101	45	105	E
F	70	00000000001000110	46	106	F
G	71	00000000001000111	47	107	G
H	72	00000000001001000	48	110	H
I	73	00000000001001001	49	111	I
J	74	00000000001001010	4a	112	J
K	75	00000000001001011	4b	113	K
L	76	00000000001001100	4c	114	L
M	77	00000000001001101	4d	115	M

Decimal**Hex****Oct****HTML**

Advanced Crypto

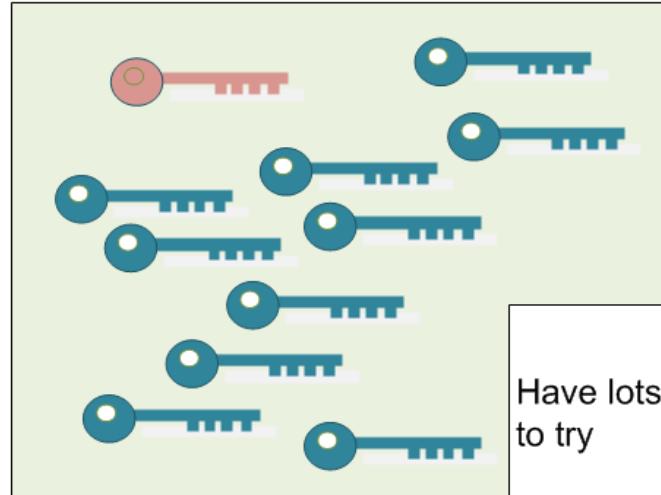
1. Ciphers and Fundamentals

Prime Numbers,
Large Numbers
and GCD



<http://asecuritysite.com/crypto>

Author: Prof Bill Buchanan

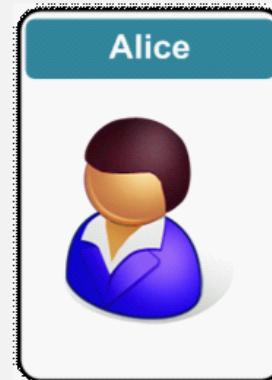


Have lots of different things to try

13,407,807,929,942,597,099,574,02
4,998,205,846,127,479,365,820,592,
393,377,723,561,443,721,764,030,0
73,546,976,801,874,298,166,903,42
7,690,031,858,186,486,050,853,753,
882,811,946,569,946,433,649,006,0
84,096



Make it mathematically difficult ... prime numbers ... and large number maths



Prime numbers are difficult to factorize

2, 3, 5, 7, 11, 13,
17, 19, 23, 29, 31, 37, ...

p
1231

q
9551

$p-1$

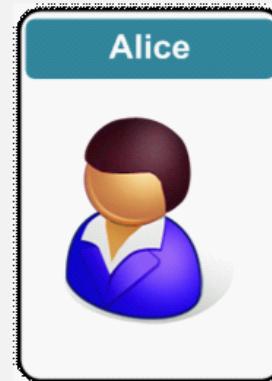
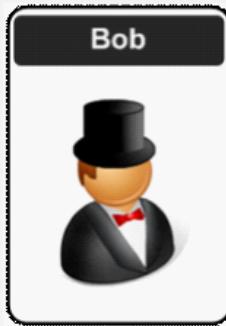
$q-1$

11,746,500

$(p-1)(q-1)$

Primes of 12?





In cryptography we often find the Greatest Common Denominator (GCD)

42, 56

Factors:

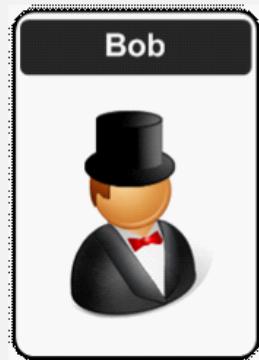
2

14

GCD

GCD of 12, 30?





32,317,006,071,311,007,300,714,876,688,669,951,960,444,102,669,715,484,032,130,345,427,524,655,138,867,890,893,197,201,411,522,9
13,463,688,717,960,921,898,019,494,119,559,150,490,921,095,088,152,366,448,283,120,630,877,367,300,996,091,750,197,750,389,652,1
06,796,057,638,384,067,568,276,792,218,642,619,756,161,838,094,338,476,170,470,581,645,852,036,305,042,887,575,891,541,065,808,6
07,552,399,123,930,385,521,914,333,389,668,342,420,684,974,786,564,569,494,856,176,035,326,322,058,077,805,659,331,026,192,708,4
60,314,150,258,592,864,177,116,725,943,603,718,461,857,357,598,351,152,301,645,904,403,697,613,233,287,231,227,125,684,710,820,2
09,725,157,101,726,931,323,469,678,542,580,656,697,935,045,997,268,352,998,638,215,525,166,389,437,335,543,602,135,433,229,604,6
45,318,478,604,952,148,193,555,853,611,059,596,230,656



Cryptography uses Big
Integers ... 512 bits,
1,024 bits, 2,048 bits ...

2,048 bit integer

Bits Max value

16 65,536

32 4,294,967,296

48 281,474,976,710,656

64 18,446,744,073,709,551,616

80 1,208,925,819,614,629,174,706,176

96 79,228,162,514,264,337,593,543,950,336

112 5,192,296,858,534,827,628,530,496,329,220,096

128 340,282,366,920,938,463,463,374,607,431,768,211,456

144 22,300,745,198,530,623,141,535,718,272,648,361,505,980,416

160 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,97 6

176 95,780,971,304,118,053,647,396,689,196,894,323,976,171,195,136,4 75,136

192 6,277,101,735,386,680,763,835,789,423,207,666,416,102,355,444,46 4,034,512,896

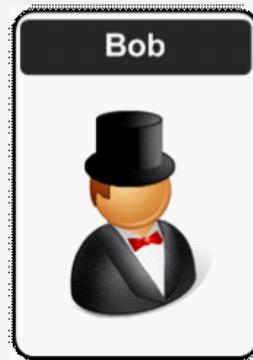
208 411,376,139,330,301,510,538,742,295,639,337,626,245,683,966,408, 394,965,837,152,256

224 26,959,946,667,150,639,794,667,015,087,019,630,673,637,144,422,5 40,572,481,103,610,249,216

240 1,766,847,064,778,384,329,583,297,500,742,918,515,827,483,896,87 5,618,958,121,606,201,292,619,776

Typical sizes of integers





Pseudo-Random Number Generators (PRNGs). Repeat after a given time. Fast. Deterministic. Periodic.

True Random Number Generators (TRNGs). True random eg keystroke analysis. Slow. Non-deterministic. Aperiodic.

Lotteries and Draws	TRNG
Games and Gambling	TRNG
Random Sampling	TRNG
Simulation and Modelling	PRNG
Security	TRNG

192-bit random:

8aa209c1432e25840857fbe82675299083009a327332181
63f2787cf8e50a1d3d8388b4864b36d70ae52304412788aa
7799a53155755e06b3d7afc8118f2bbde1993f07ef169f1c
...

128-bit random:

YSITF-RKRTC-KZUBW-FBQLF-YZZHL-VTQAQ-QTTWI-AUGYI-FVTEP-LKDAZ-APIVE-PSCZZ
WQMZH-VRYLS-IUJAE-AQWJT-AWJPY-KCVMH-AUVPY-OFDNC-DNPGY-EAQCA-GRFKK-FYLSF



Bob



CRC-32 Example

[\[Back\]](#) CRC is one of the most reliable error detection schemes and can detect up to 99.5% of all errors. The most commonly used code is the CRC-32 standard code which is defined by the CCITT, and will give a 32-bit CRC signature (8 hex characters). This signature is normally appended onto the data, and then checked when the data is read. If the CRC-32 check differs from the stored value, there is likely to be an error in the data. [\[Theory\]](#) [\[Background\]](#)

The basic idea of a CRC can be illustrated using an example. Suppose the transmitter and receiver were both to agree that the numerical value sent by the transmitter would always be divisible by 9. Then should the receiver get a value which was not divisible by 9 it would know it knows that there had been an error. For example, if a value of 32 were to be transmitted it could be changed to 320 so that the transmitter would be able to add to the least significant digit, making it divisible by 9. In this case the transmitter would add 4, making 324. If this transmitted value were to be corrupted in transmission then there would only be a 10% chance that an error would not be detected.

The quick brown fox jumps over the lazy dog

Message:

The quick brown fox jumps over the lazy dog

Generate CRC-32

The results are then:

414fa339

414fa339

CRC-32

Examples

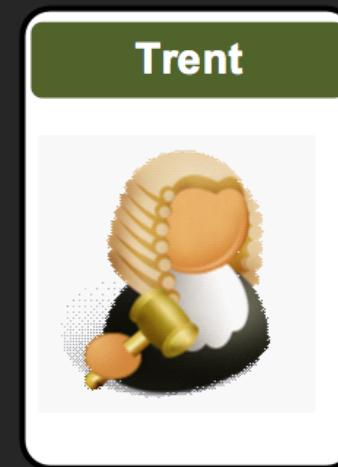
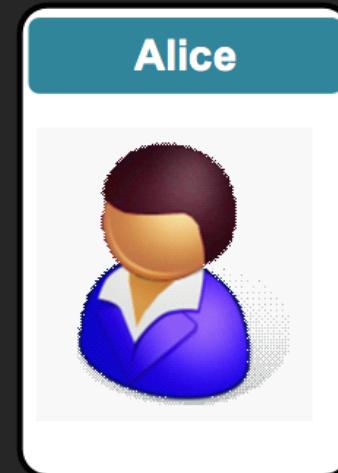
- * Try "The quick brown fox jumps over the lazy dog". [Try!](#), which should give a CRC-32 value of: 414fa339 [Check](#)
- * Try "Test vector from febooti.com". [Try!](#), which should give a CRC-32 value of: 0c877f61 [Check](#)
- * Try "". [Try!](#), which should give a CRC-32 value of 00000000 [Check](#)



Advanced Crypto

1. Ciphers and Fundamentals

Key-based Encryption

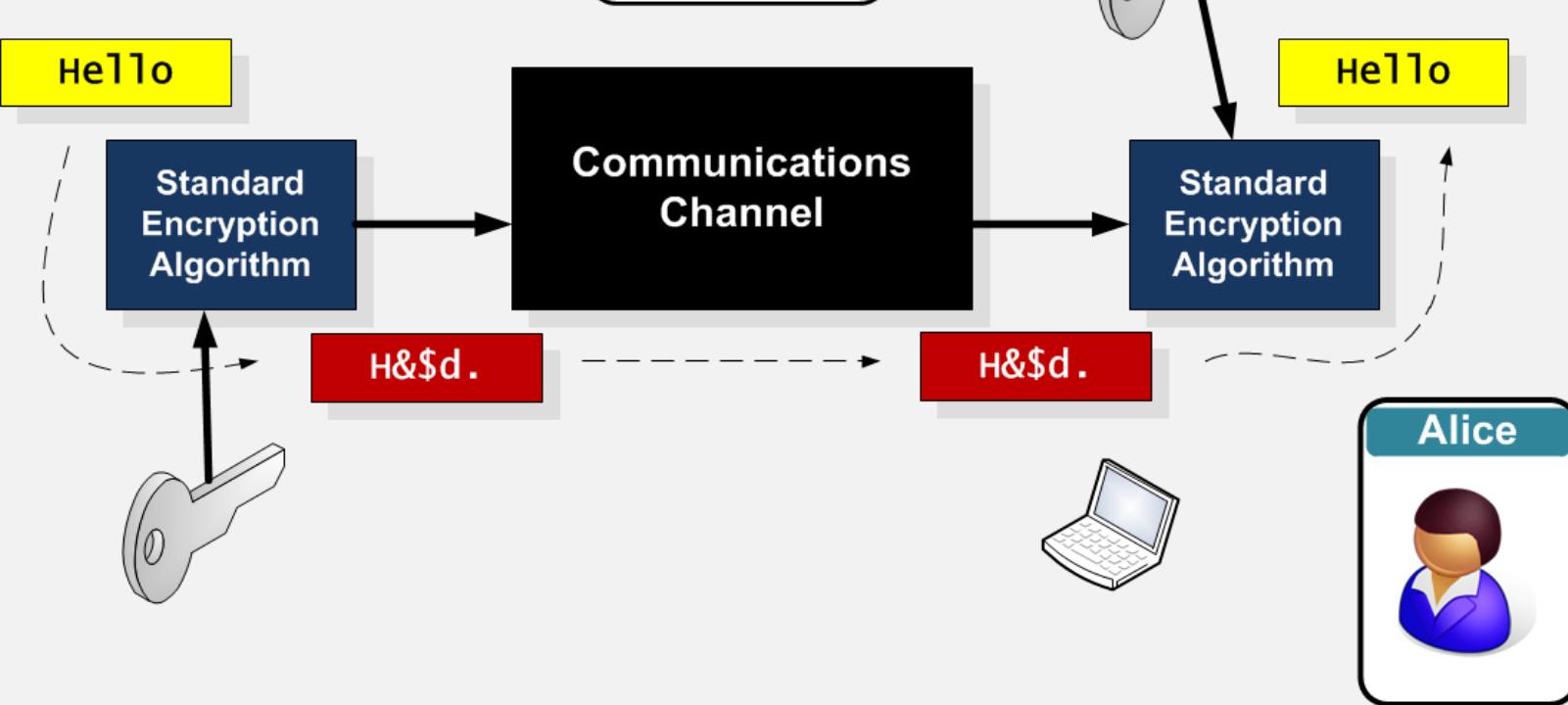


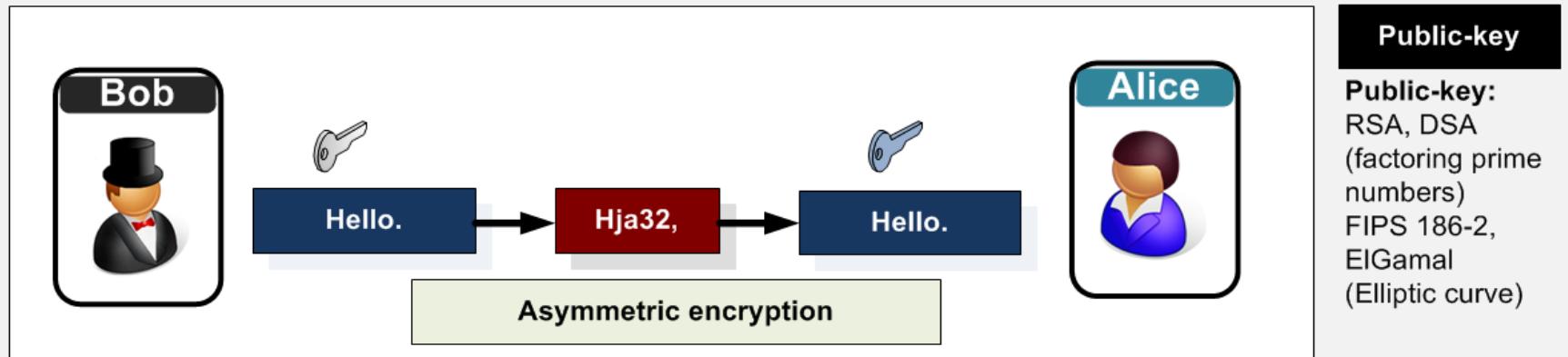
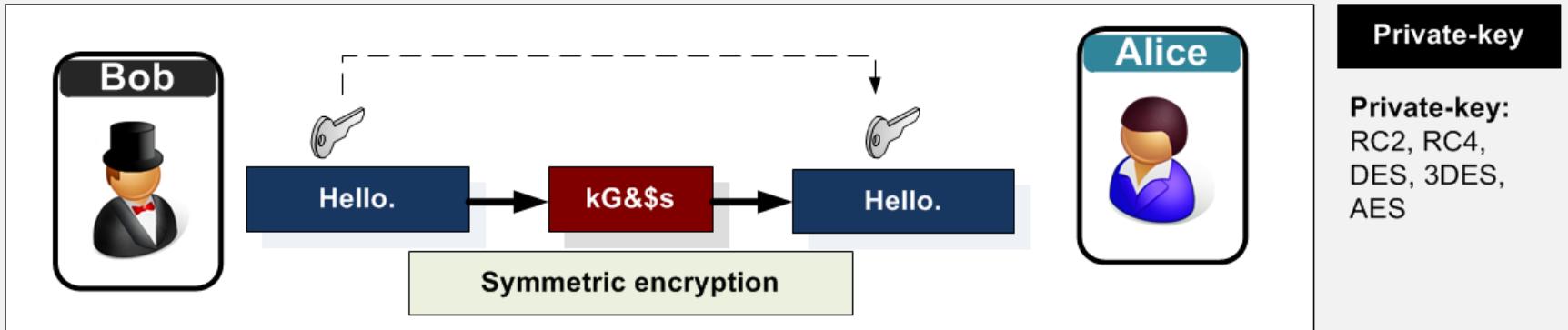
<http://asecuritysite.com/crypto>

Author: Prof Bill Buchanan



The major problem is that Eve could gain the encoding algorithm.







For example, if we have a key with four notches ... each which can exist or not ... how many keys can we have?

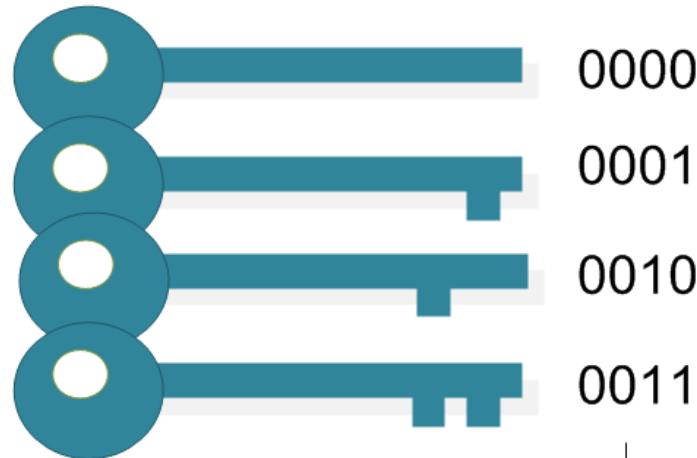
How safe is the key?

- the more keys ... the less likely it is to find the key.





**16 key
combinations**
2 to the power of 4
(2^4)





Number of keys

The larger the key, the greater the key space.

Code size	Number of keys	Code size	Number of keys	Code size	Number of keys
1	2	12	4,096	52	4.5×10^{15}
2	4	16	65,536	56	7.21×10^{16}
3	8	20	1,048,576	60	1.15×10^{18}
4	16	24	16,777,216	64	1.84×10^{19}
5	32	28	2.68×10^8	68	2.95×10^{20}
6	64	32	4.29×10^8	72	4.72×10^{21}
7	128	36	6.87×10^{10}	76	7.56×10^{22}
8	256	40	1.1×10^{12}	80	1.21×10^{24}
9	512	44	1.76×10^{13}	84	1.93×10^{25}
10	1024	48	2.81×10^{14}	88	3.09×10^{26}



Cryptography Fundamentals

Traditional ciphers.

Frequency Analysis.

Operators and GCD.

Encoding.

Big Integers.

Random Numbers.

Key-based Encryption.

Prof Bill Buchanan OBE

<http://asecuritysite.com/encryption>



LiveSlides web content

To view

Download the add-in.

liveslides.com/download

Start the presentation.