

Crypto Foundations



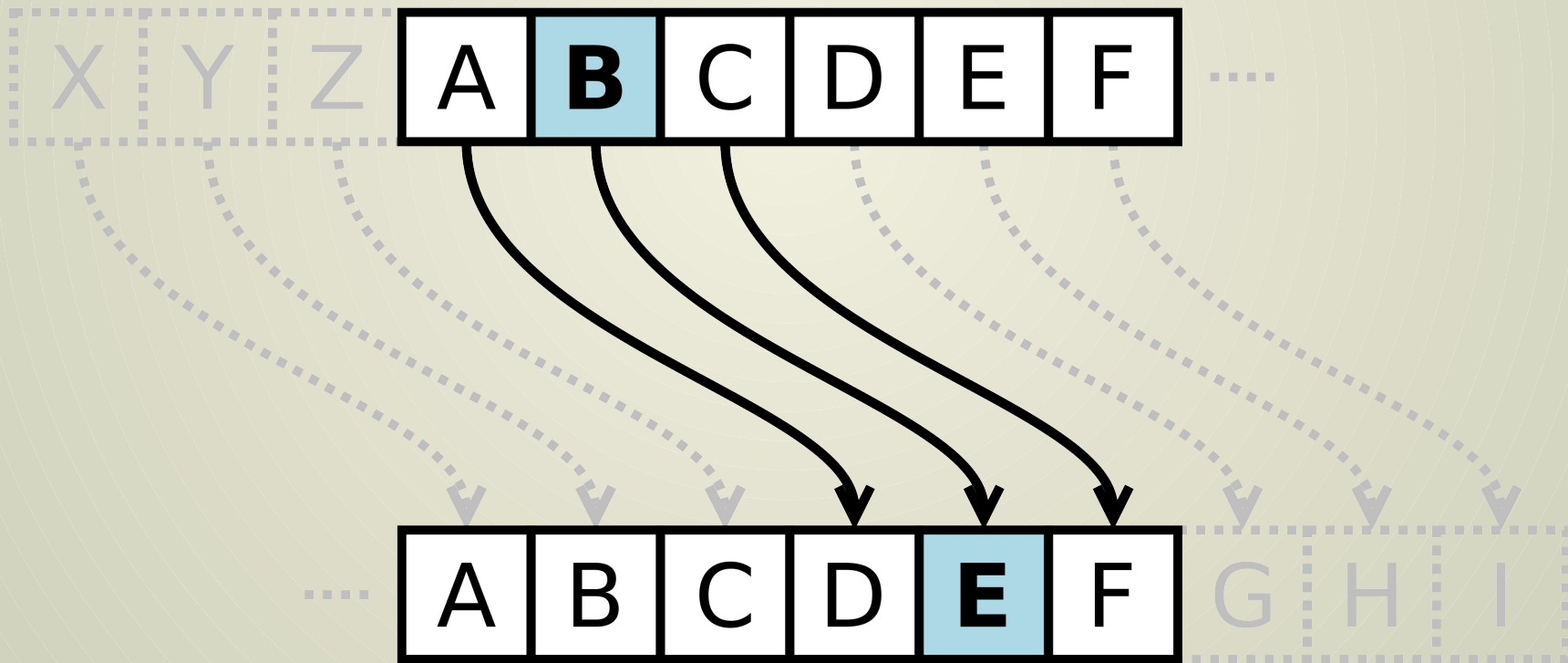
By Chad Parry <chad.parry@overstock.com>

Overstock.com Tech Day 9/2012

Security Over Time



Caesar Cipher



Substitution Cipher

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	

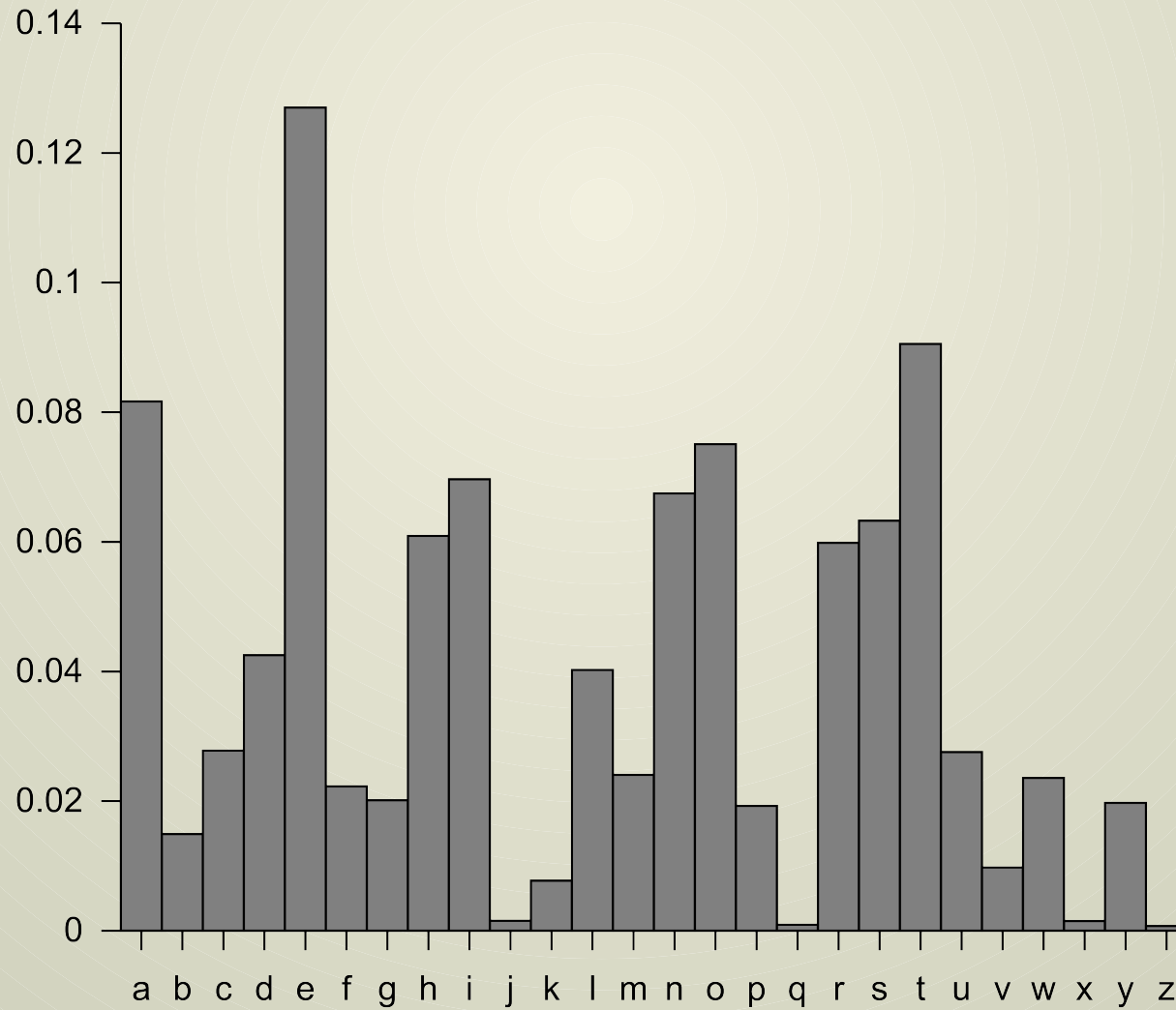
>
X

⌈·⌋ ⌋⌈ ⌈·⌋ ⌋⌈ V
M A R K S

> ⌈⌋ ⌈⌋
T H E

V ⌈·⌋ ⌈·⌋ >
S P O T

Frequency Analysis



Vigenère cipher

	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

Plaintext: ATTAC KATDA WN

Key: LEMON LEMON LE

Ciphertext: LXFOP VEFRN HR

Kasiski Examination

Plaintext: CRYPT OISSH ORTFO RCRYP TOGRA PHY
Key: ABCDA BCDAB CDABC DABCD ABCDA BCD
Ciphertext: **CSAST** **P**KVSI QUTGQ U**CSAS** **TP**IUA QJB



1234

CSAS

TPKV

SIQU

TGQU

CSAS

TPIU

AQJB

Kerckhoffs's Principle

“The enemy knows the system.”

— Claude Shannon

The only secrets should be the keys.

Security Through Obscurity

You aren't as creative as you think you are.



Steganography

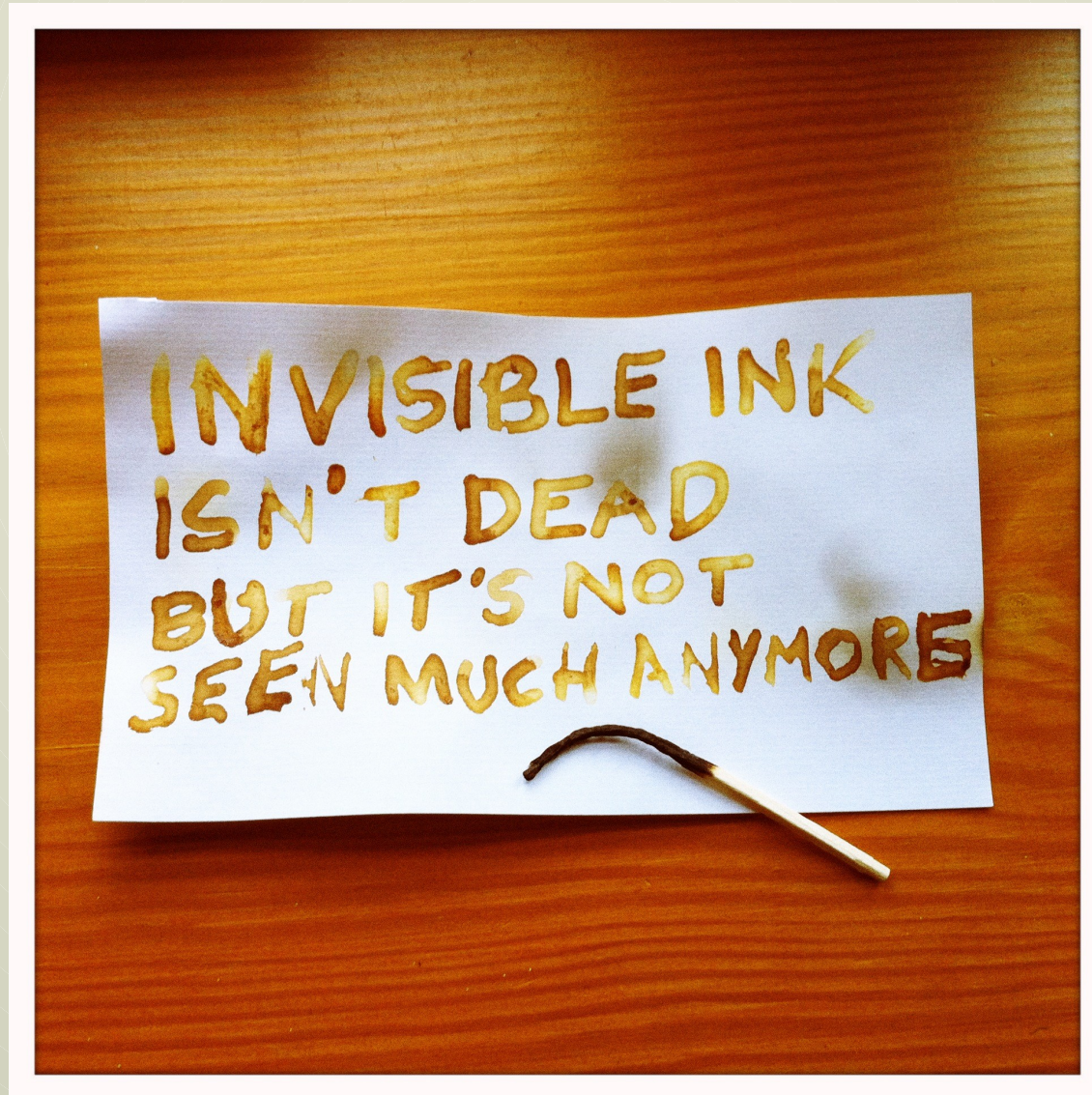


Image by John V Willshire

Automated Cryptanalysis

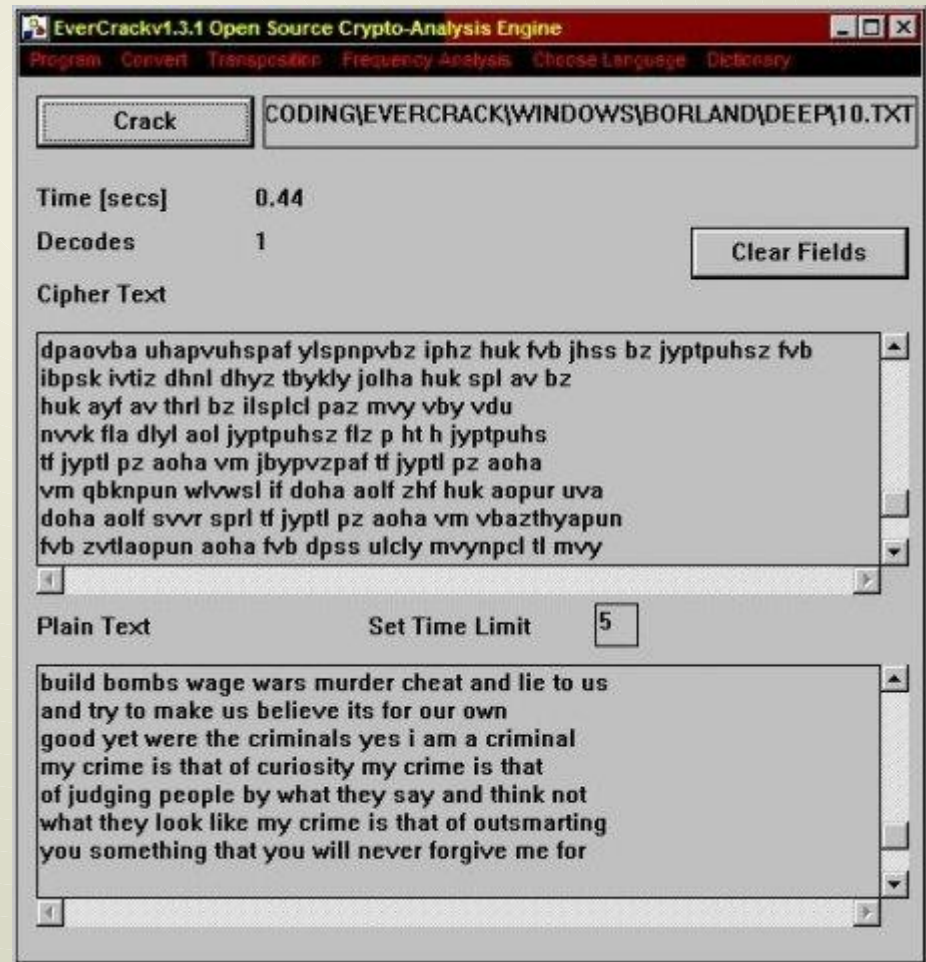
```
67 shell
C:\CODING\EVERCR~1\WINDOWS\DOS\bin>evercrack 3.txt

Cipher Text
1 18 21##110 21##13$ 14% 1 =$$ 1 27^#5 1508 ^6
08 3^(48580$4 7$5$ 14 %$6143$ ^6 &851448 8^( 71v$ 3^0$
&^ 61)7& 1* 65$5 0$4 14% 65$5 014 8^( 15$
2718 21## 8^( %^ 21&7^( 6 65$5%0 21## 8^( 61)7& &2^
&7^(=14% 1)114^& &54 &7$ v$85$14 ^7^(65% 4^ 2$ 21## 5(4
14% #1v$ 8$= 21##13$ ^7^(65% 9130 61)7& 14% 8^( @18
%1$ 5(4 14% 8^( 21## #1v$ 1& #51^& 1271#5 14%
%814) 14 8^(5 9$% @148 8$15= 65^0 4^2 2^(#% 8^(
9$ &^ &51%5 1## &7$ %18= 65^0 &71* %18 &^
&71& 6^5 ^4$ 37143$ j(^& ^4$ 37143$ &^ 3^0$ 9130
7$5$ 1* 8^(4) 0$4 14% &5## ^5 $4$01$= &71& &7$8
018 &10$ ^5 #1v$= 9(& &7$8 21## 45v$5 &10$ ^5
65$5%0

[1]i am william wallace and i see a whole army of
my countrymen here in defiance of tyranny you have come
to fight as free men and free man you are
what will you do without freedom will you fight two
thousand against ten the veteran shouted no we will run
and live yes wallace shouted back fight and you may
die run and you will live at least awhile and
dying in your bed many years from now would you
be to trade all the days from this day to
that for one chance just one chance to come back
here as young men and tell our enemies that they
may take our lives but they will never take our
freedom

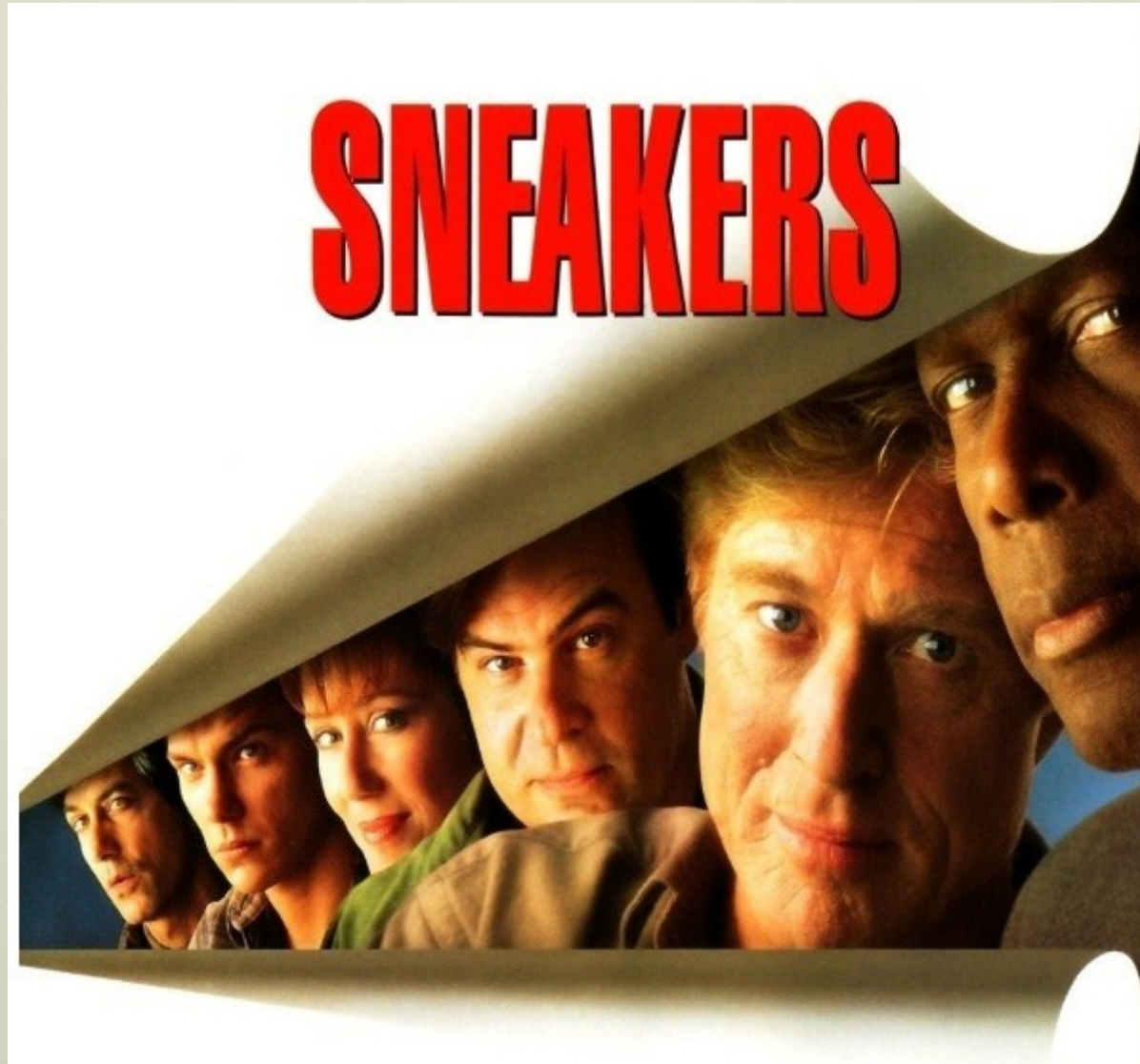
Time [secs]: 0.270000
Decodes: 1
EverCrackv1.1.2 Open Source Crypto-Analysis Engine
Developer: Cory Michael Boston [Dark Logic]

C:\CODING\EVERCR~1\WINDOWS\DOS\bin>
```



Shown here: <http://sourceforge.net/projects/evercrack/>

Modern Cryptography



One-Time Pad

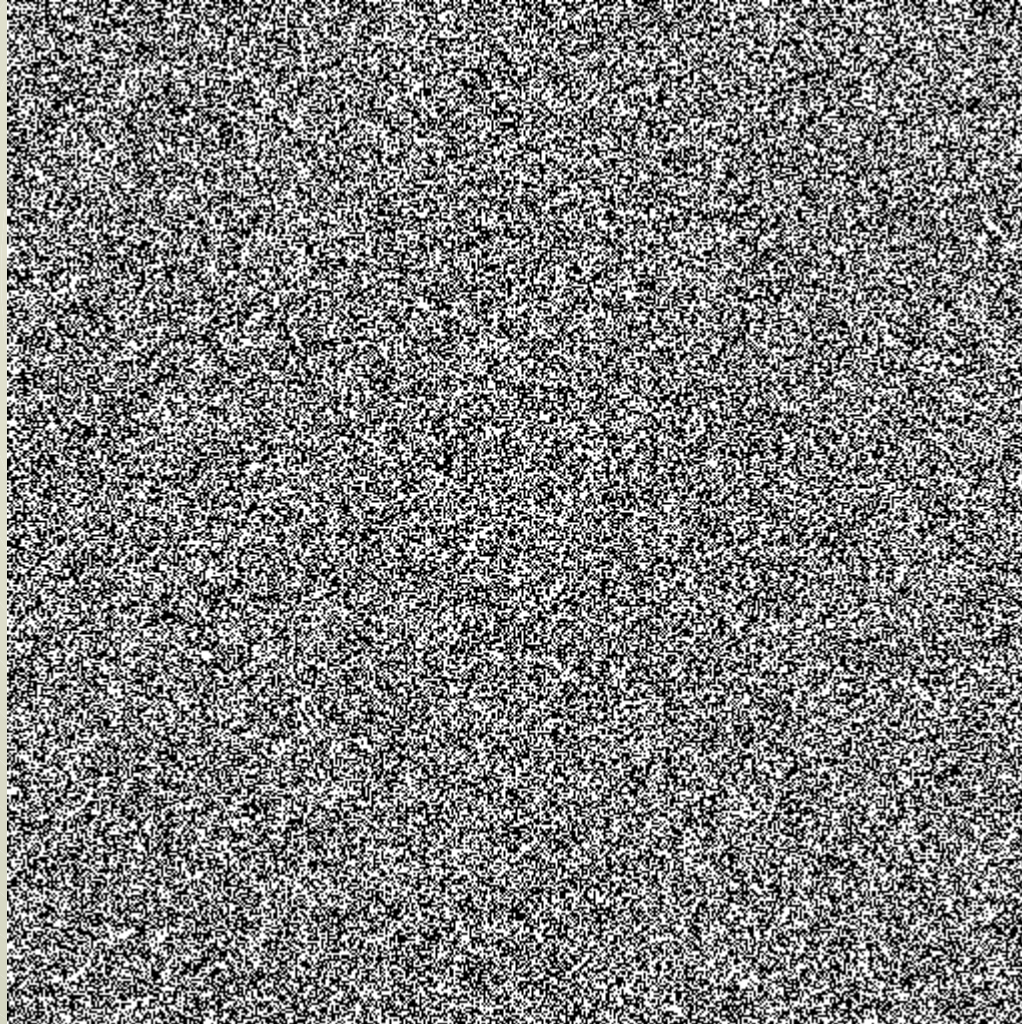


Image by Bo Allen

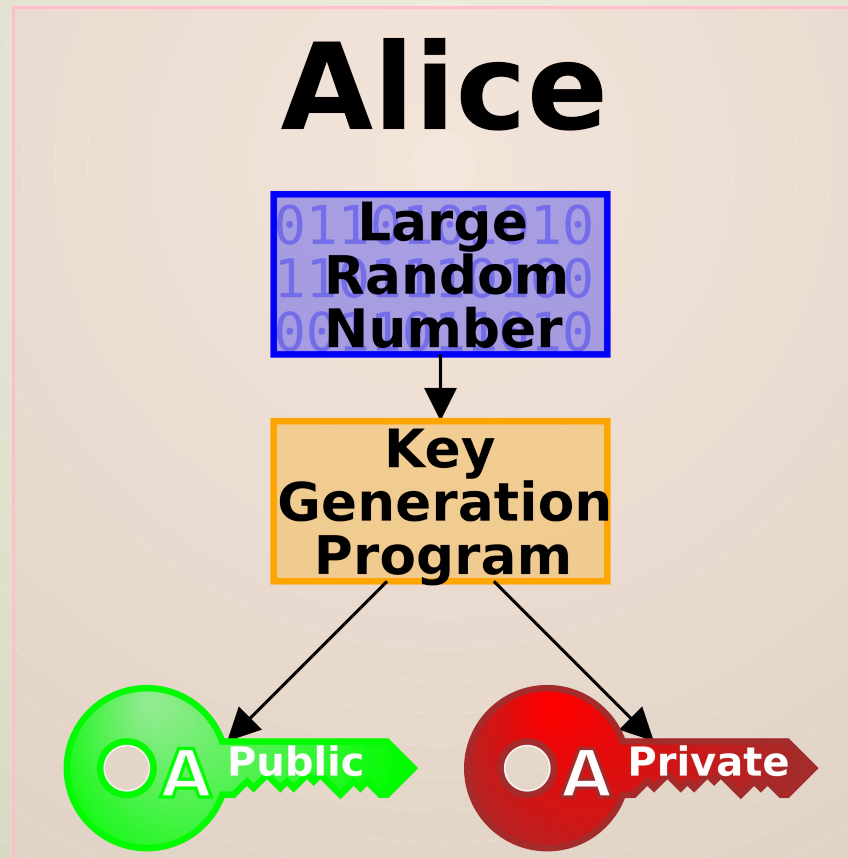
One-Time Pad Instructions

- ♦ Generate random numbers for key, *perfectly safely*.
- ♦ Exchange key with recipient, *perfectly safely*.
- ♦ Encrypt plaintext by addition with key.
- ♦ Dispose of key, *perfectly safely*.

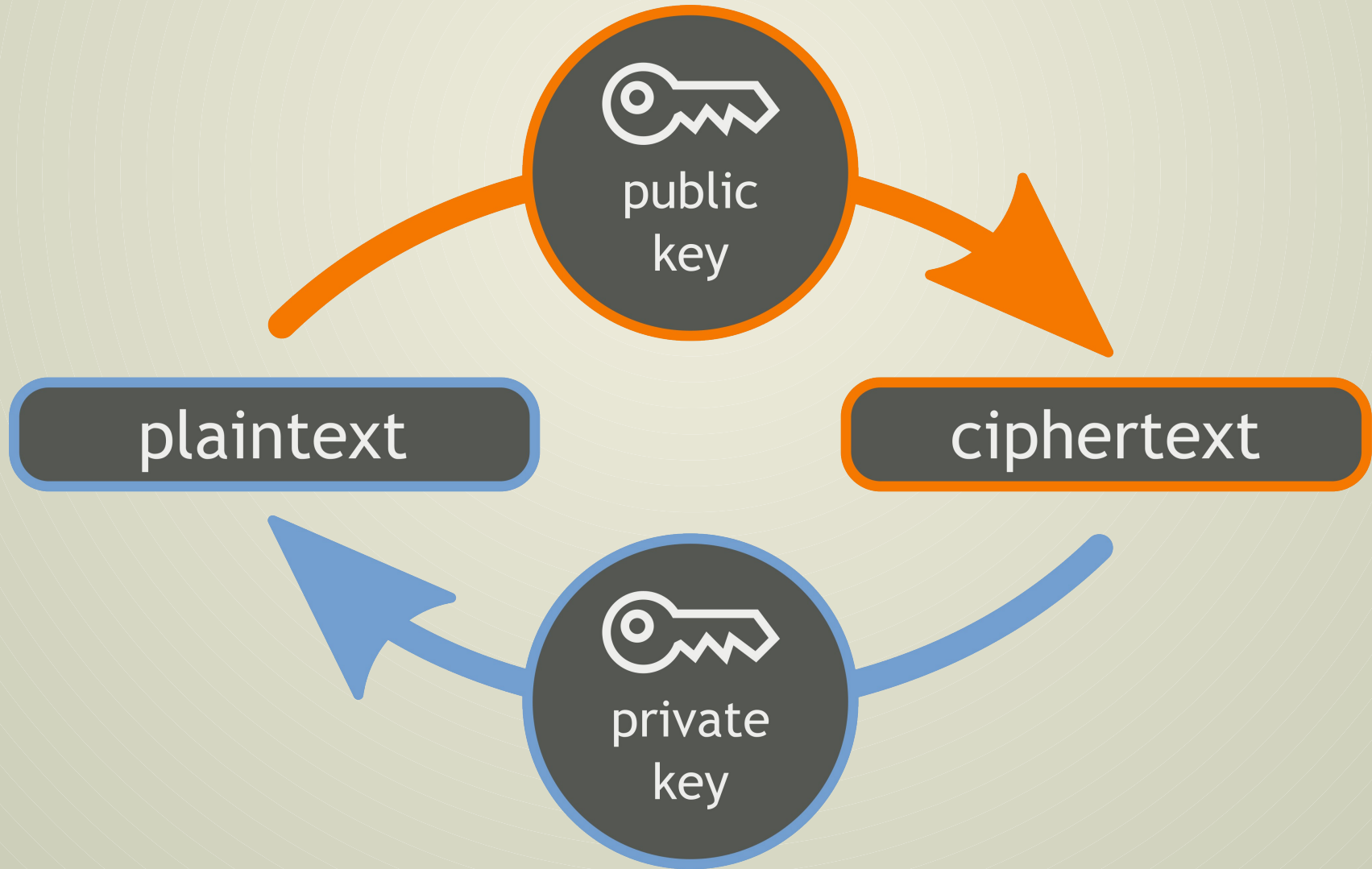
Venona Project



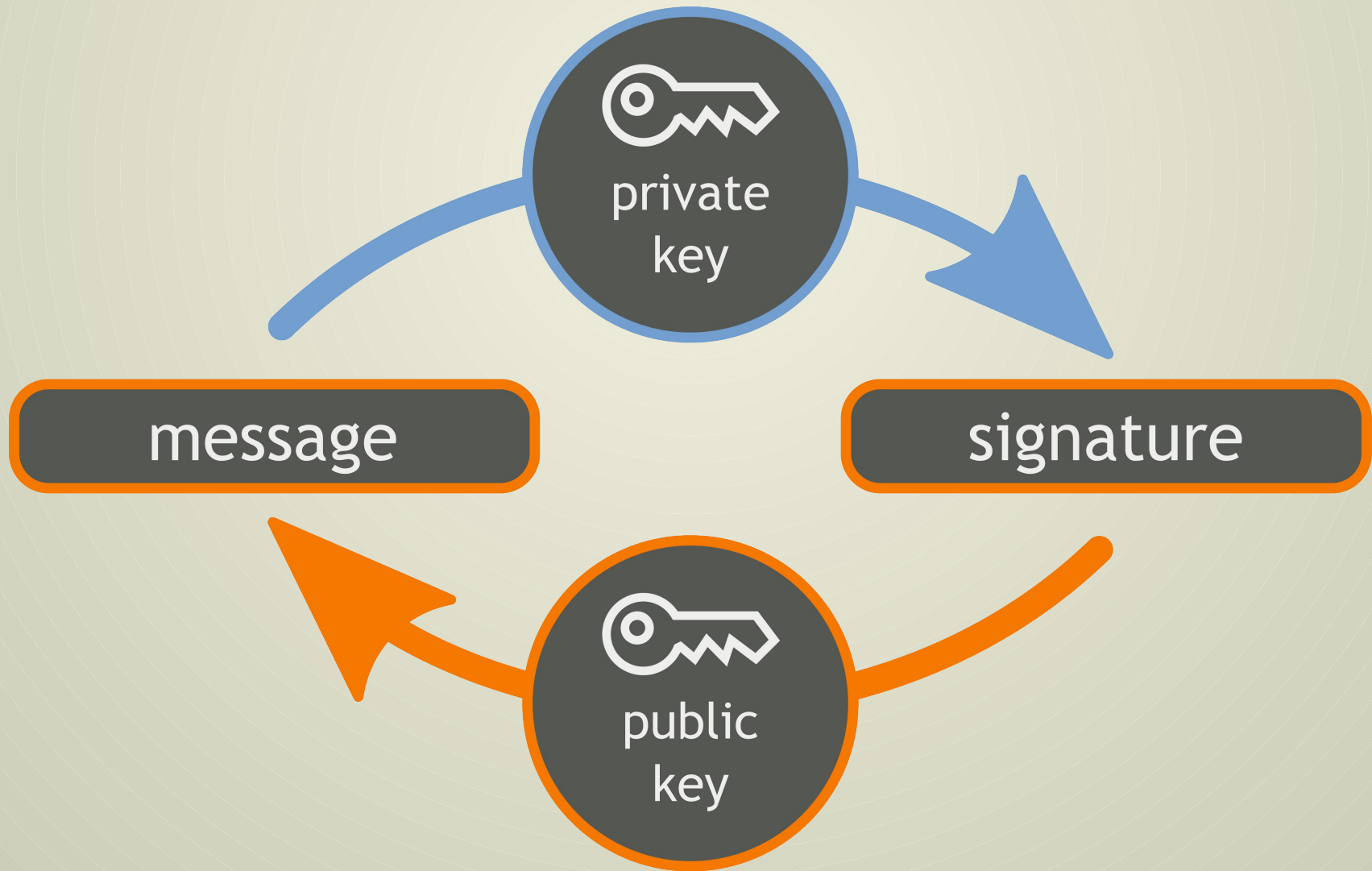
Asymmetric Keys



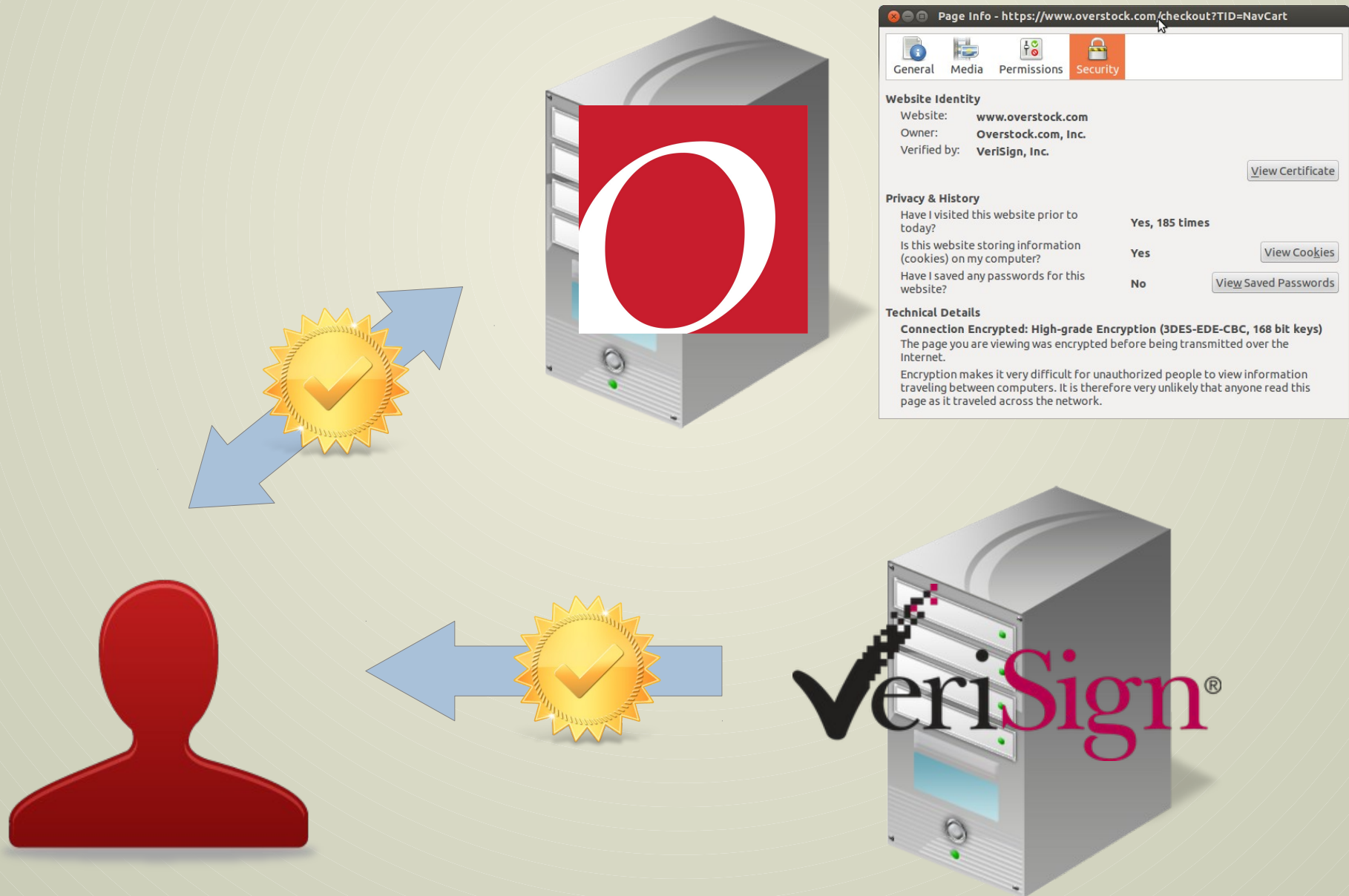
Public-Key Encryption



Public-Key Signing



Shopping Authentication



RSA Key Example

- ♦ Choose random primes: $p = 137, q = 131$
- ♦ Calculate $n = pq = 17947$
- ♦ Choose small $e = 3$
- ♦ Solve for d : $de \bmod \text{lcm}(p - 1, q - 1) = 1$
 $\therefore 3d \bmod 8840 = 1$
 $\therefore d = 2947$
- ♦ Public key: $\{ n=17947, e=3 \}$
- ♦ Private key: $\{ n=17947, d=2947 \}$

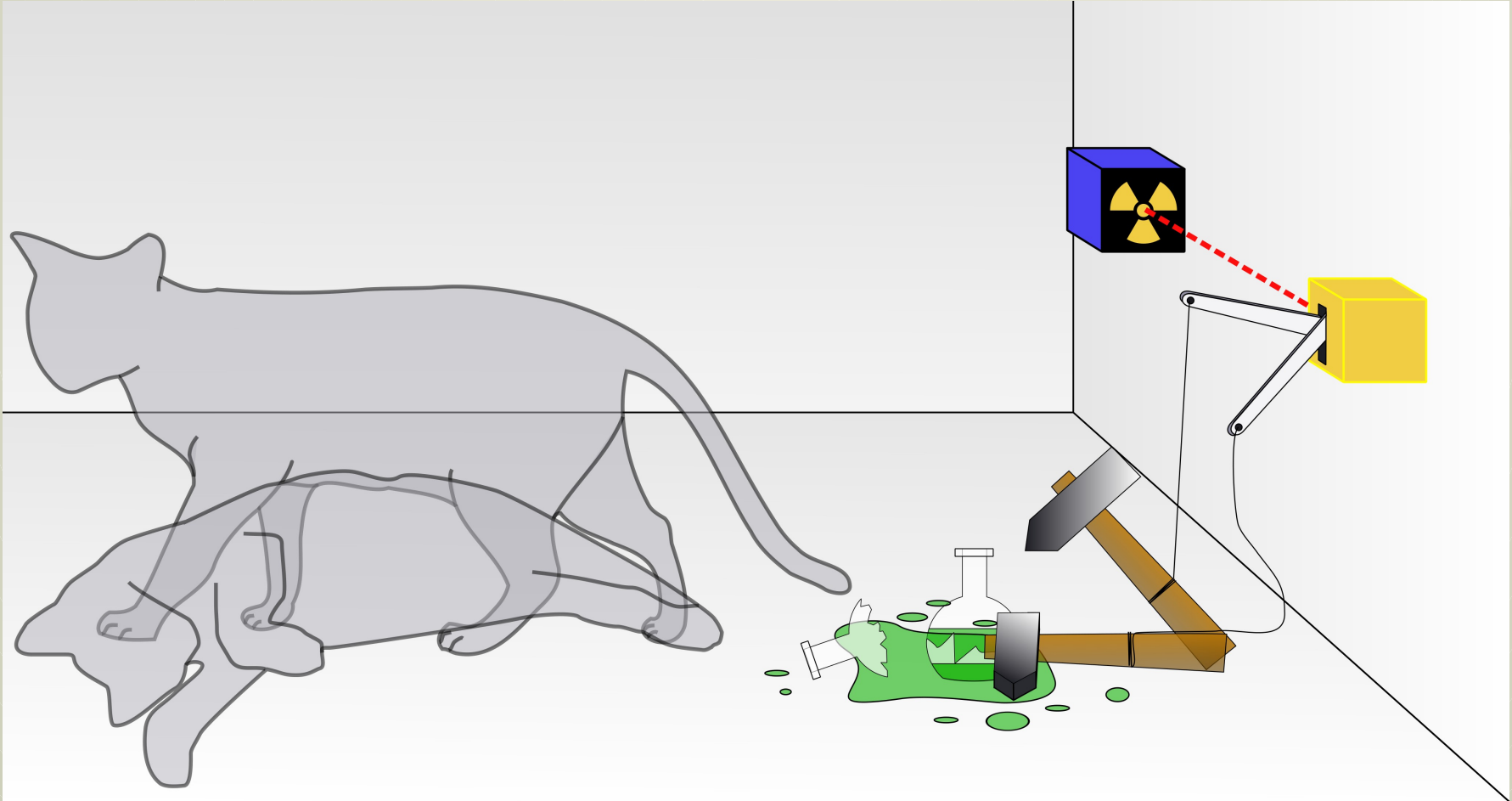
RSA Encryption Example

- Public key: $\{ n=17947, e=3 \}$
- Private key: $\{ n=17947, d=2947 \}$
- Message: $m = \text{"Hi"} \equiv [72, 105] \equiv 9321$
- Encrypt: $c = m^e \bmod n$
 $= 9321^3 \bmod 17947$
 $= 9441$
- Decrypt: $m = c^d \bmod n$
 $= 9441^{2947} \bmod 17947$
 $= 9321$

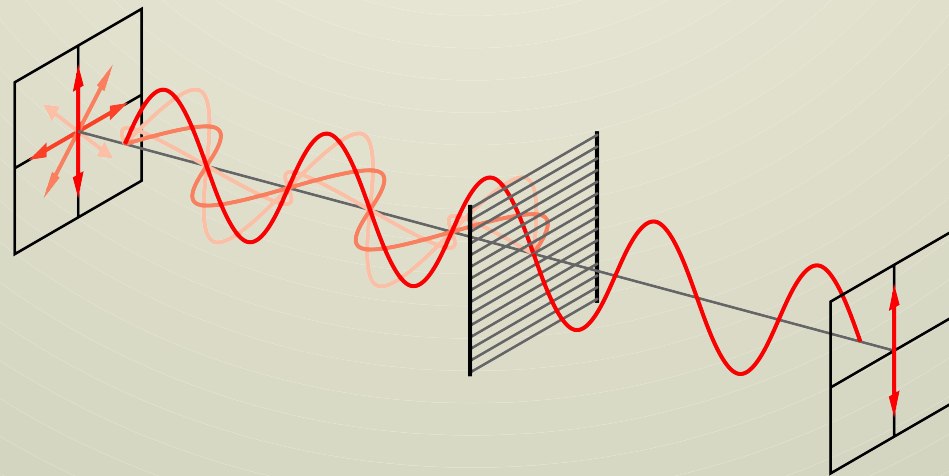
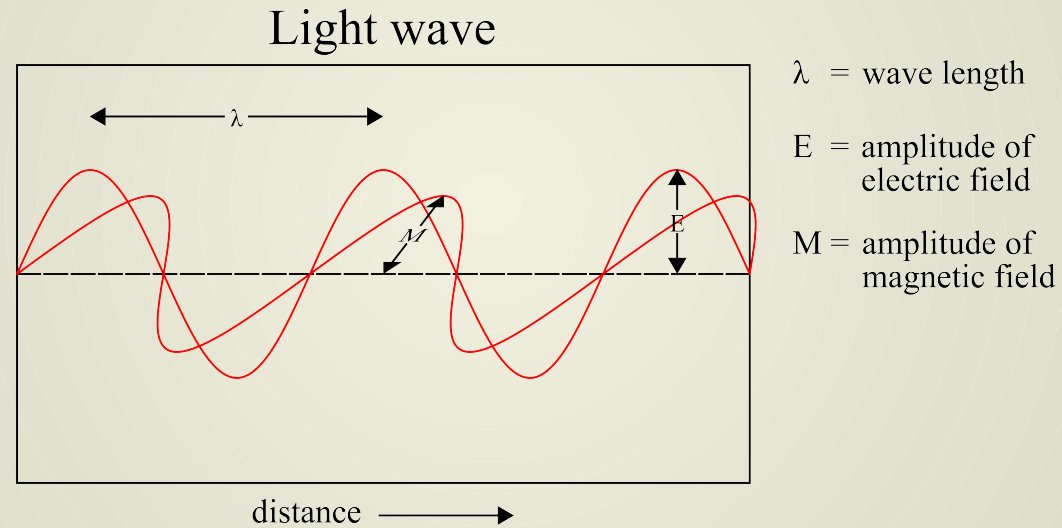
Public-Key Reliability

- ♦ Using the key incorrectly voids the warranty.
- ♦ Don't use the same key pair for both encryption and signing, unless your system gives you permission.
- ♦ The underlying factoring problem may be solvable.
- ♦ The TWINKLE device can brute-force keys.

Shor's Algorithm



Quantum Indeterminacy



Quantum Channels

Polarization	0	1
+	↑	→
×	↗	↘

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random basis	+	+	×	+	×	×	×	+
Sent polarization	↑	→	↘	↑	↘	↗	↗	→
Bob's random basis	+	×	×	×	+	×	+	+
Received polarization	↑	↗	↘	↗	→	↗	→	→
Received bit	0	0	1	0	1	0	1	1
Shared secret key	0		1			0		1

Makarov's Hack

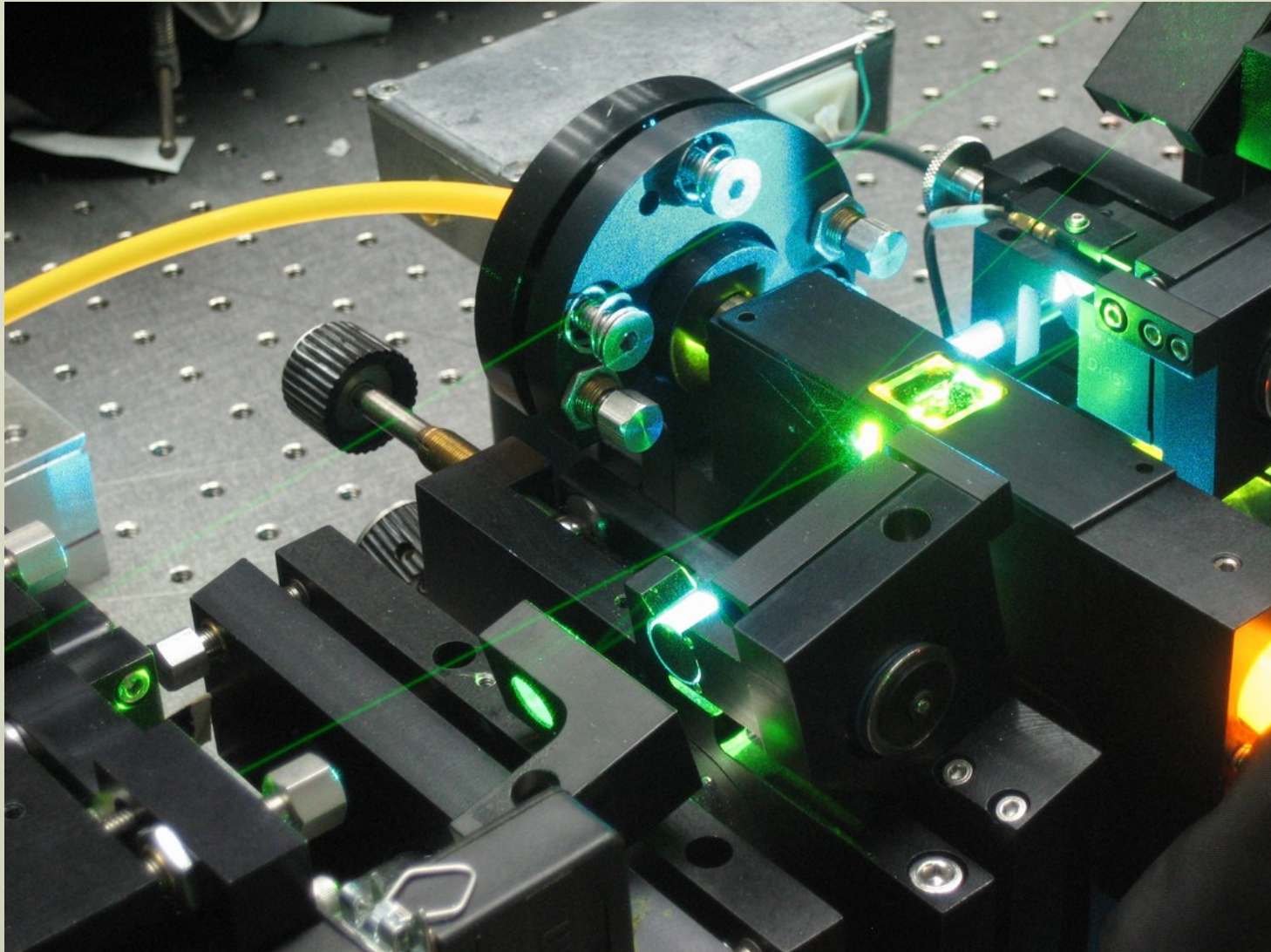


Image by "fatllama" on Flickr

Side Channel Attacks

Cryptographic proofs assume knowledge of all attack vectors.

Successful attackers will break the rules.

Acoustic Cryptanalysis



HAGELIN M-209 CIPHER MACHINE (GVG / PD)



Capacitor Hum

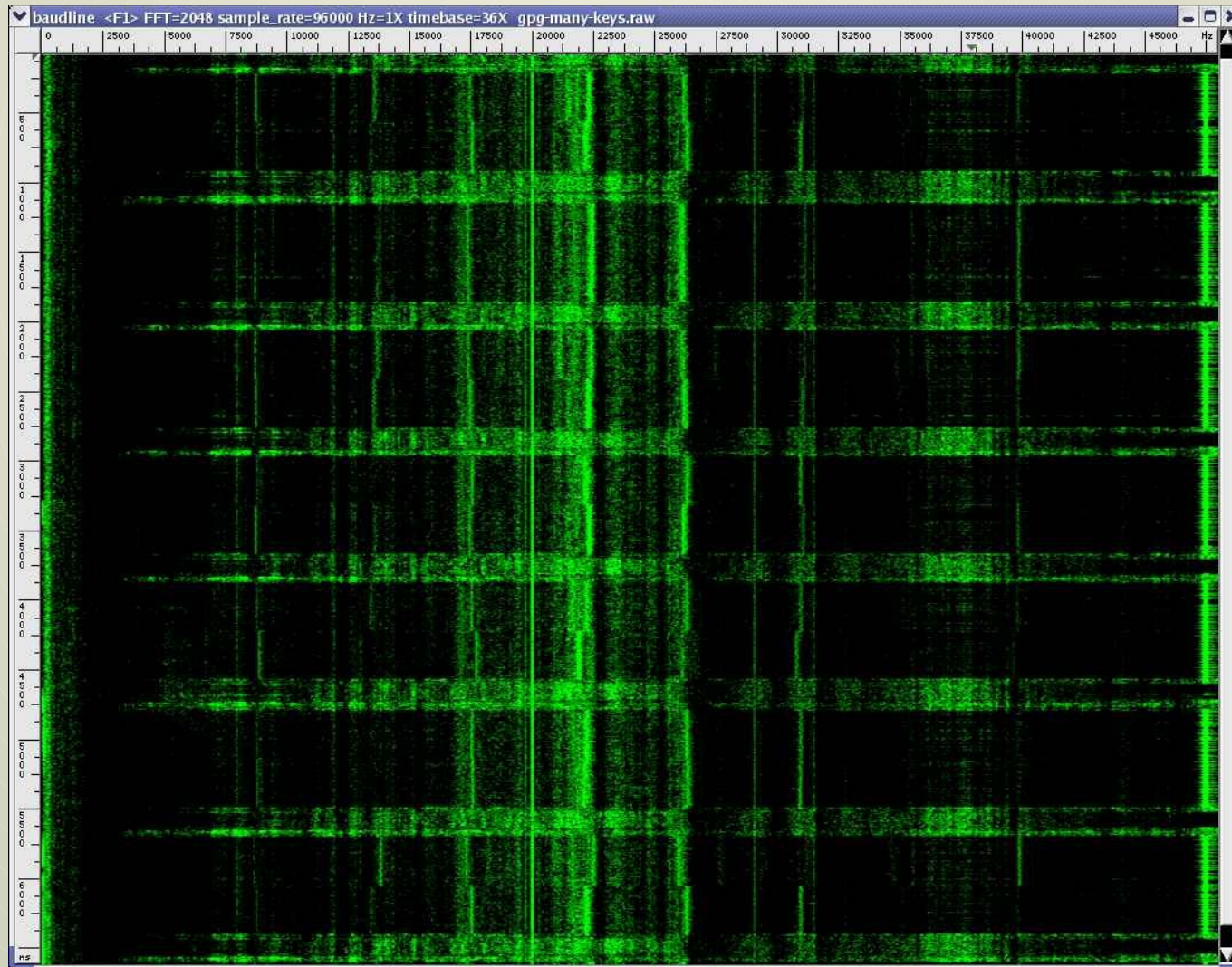


Image by Adi Shamir and Eran Tromer

Suitcase-Full-of-Money Attack



Image by "401(K) 2012" on Flickr

Overstock.com Tech Day 9/2012

Rubber-Hose Attack



Image by Sam Ley "phidauex" on Flickr

Overstock.com Tech Day 9/2012

Social Engineering



Image from <http://www.smbc-comics.com/index.php?db=comics&id=2526>

Overstock.com Tech Day 9/2012

Moral

Schneier's Law: “Any person can invent a security system so clever that she or he can't think of how to break it.”

Never invent your own cryptography.