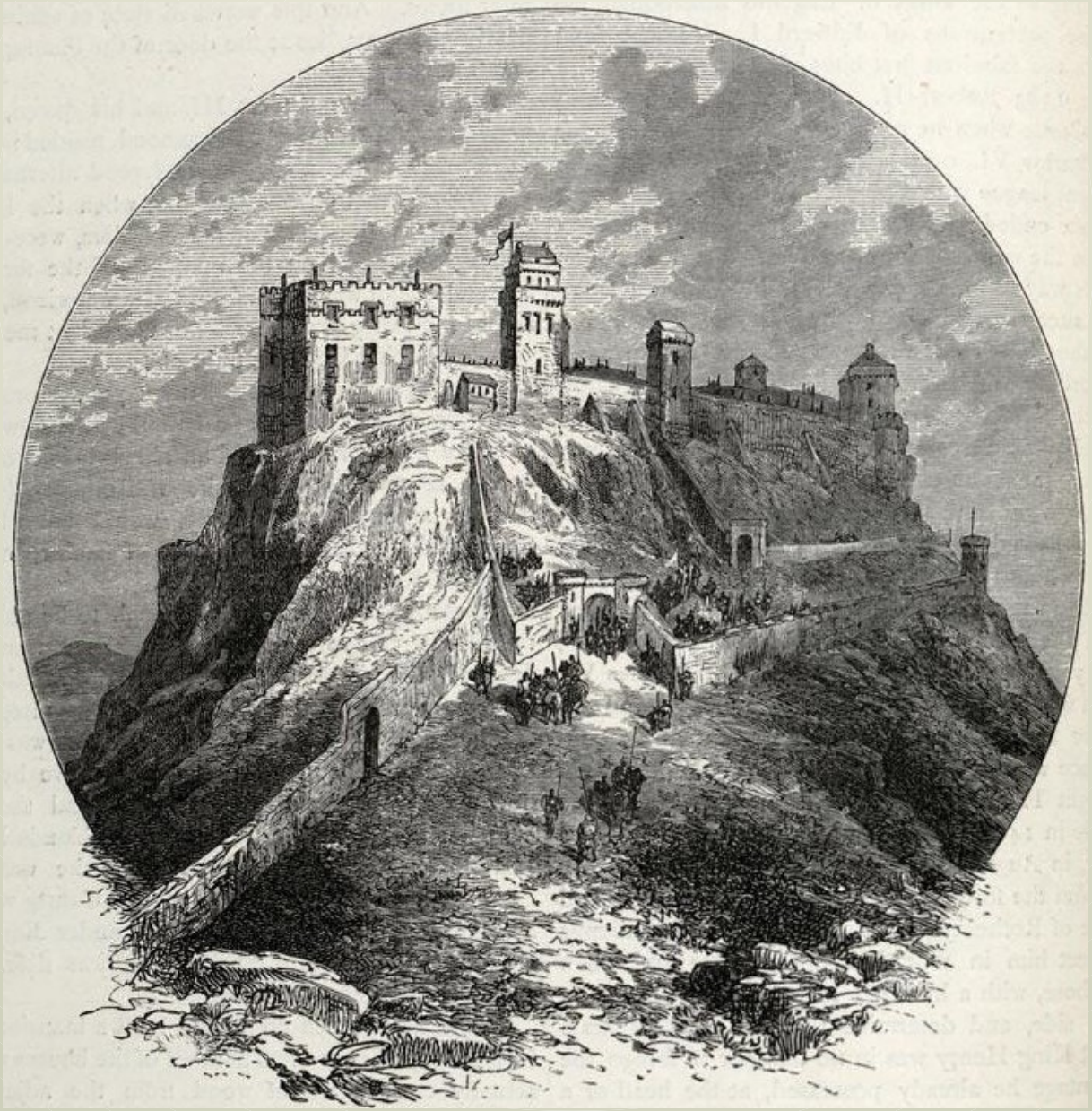
Crypto Foundations

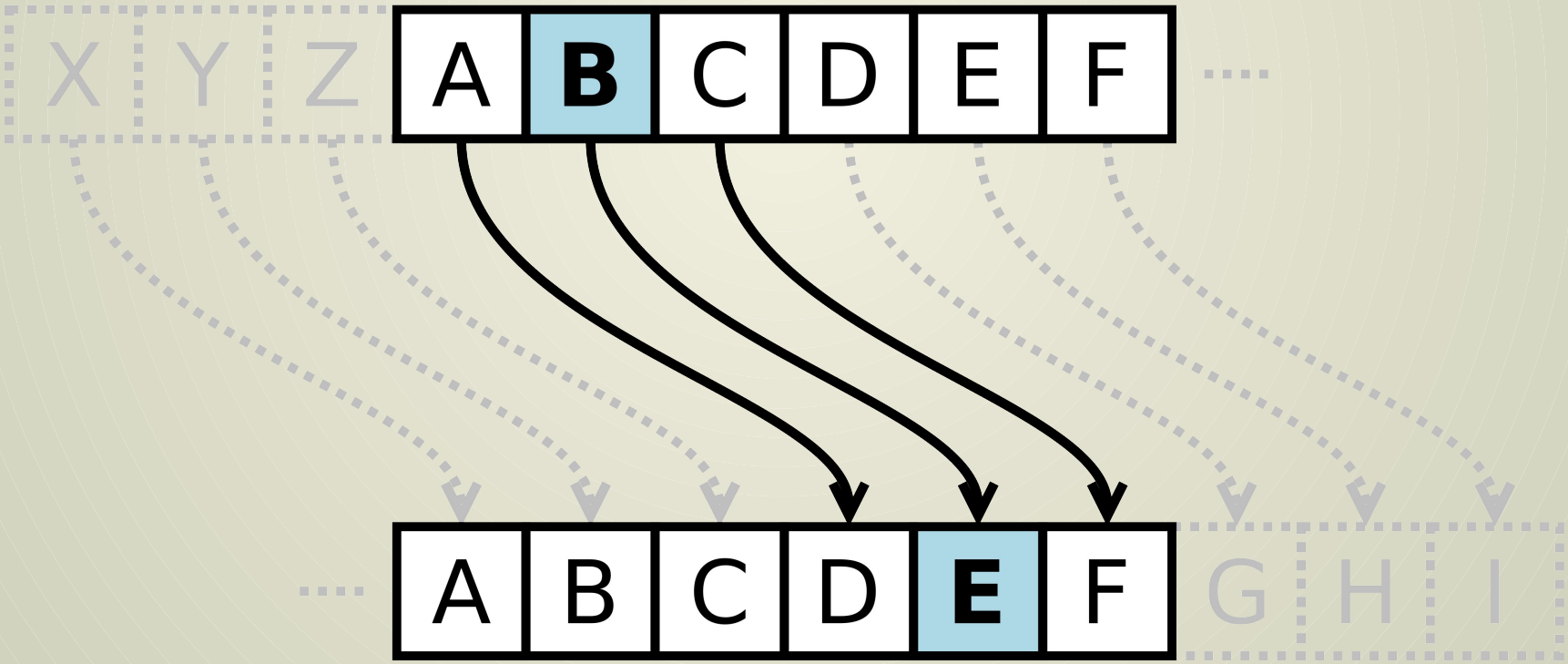
By Chad Parry <chad.parry@overstock.com>

Overstock.com Tech Day 9/2012

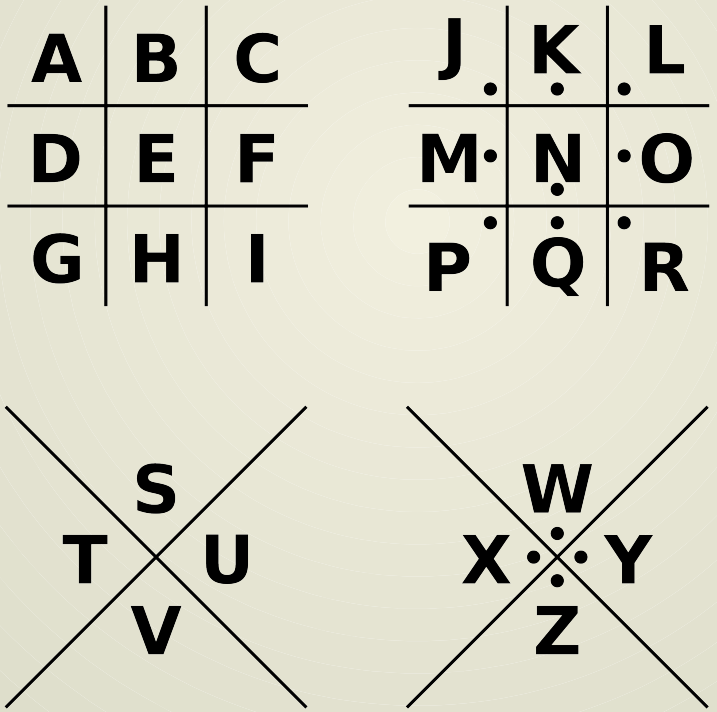
Security Over Time

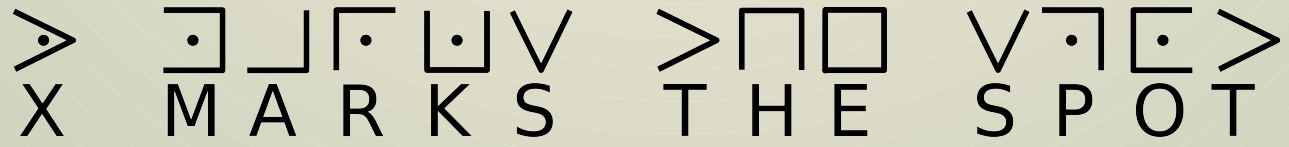


Caesar Cipher

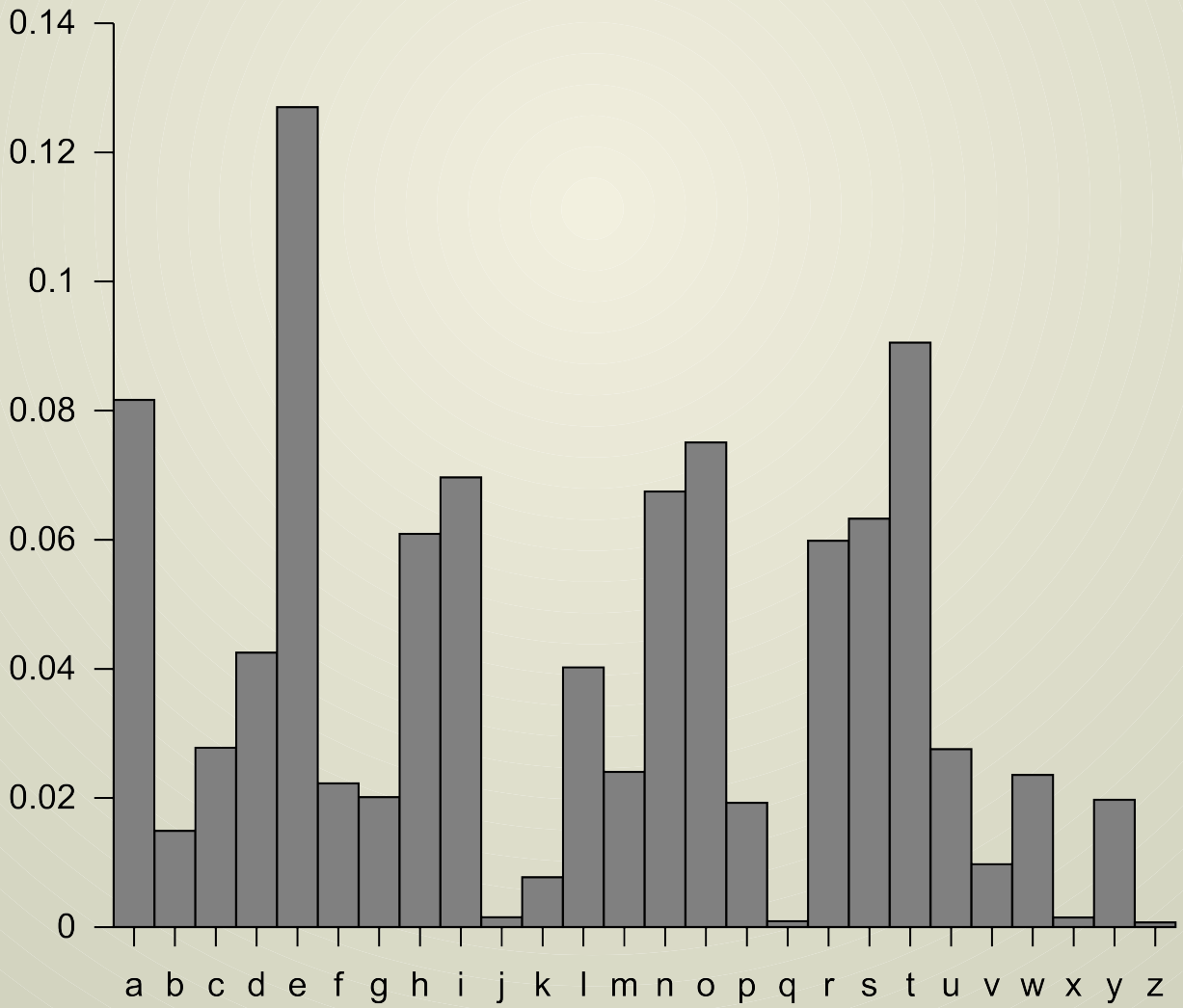


Substitution Cipher





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

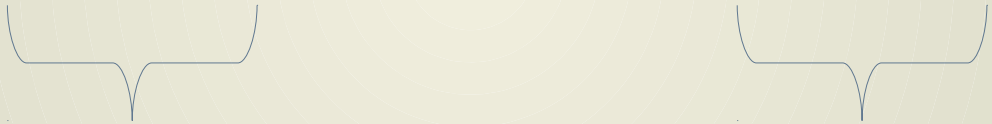
Plaintext: ATTAC KATDA WN

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

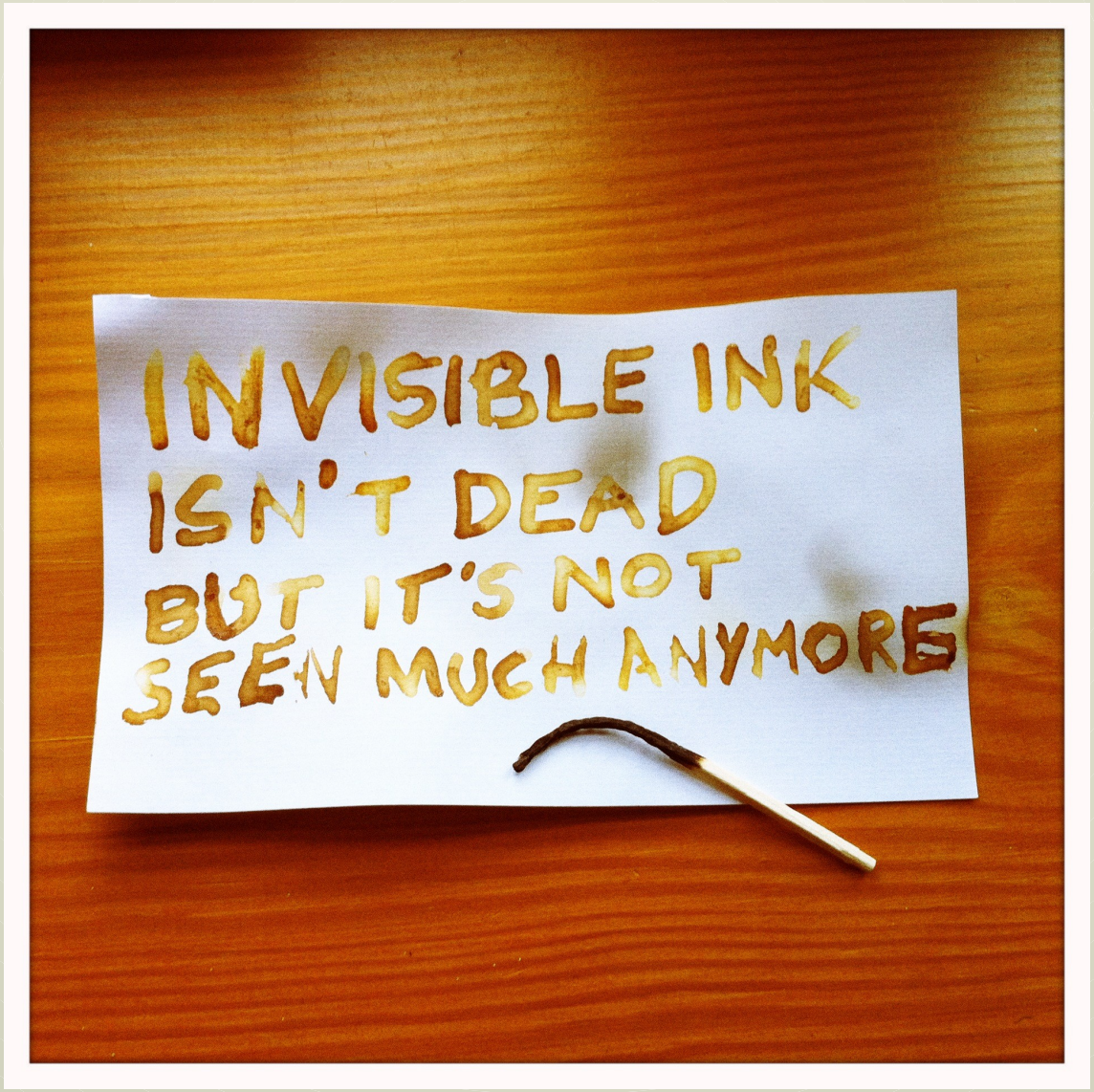
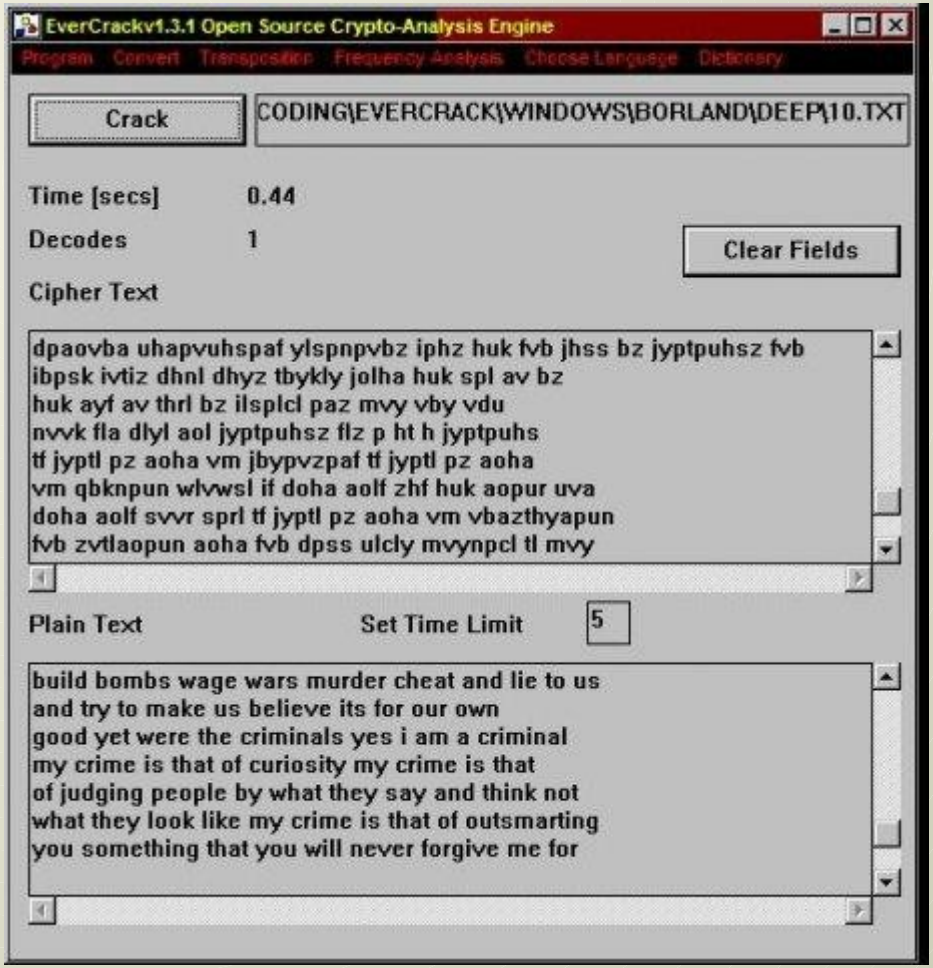


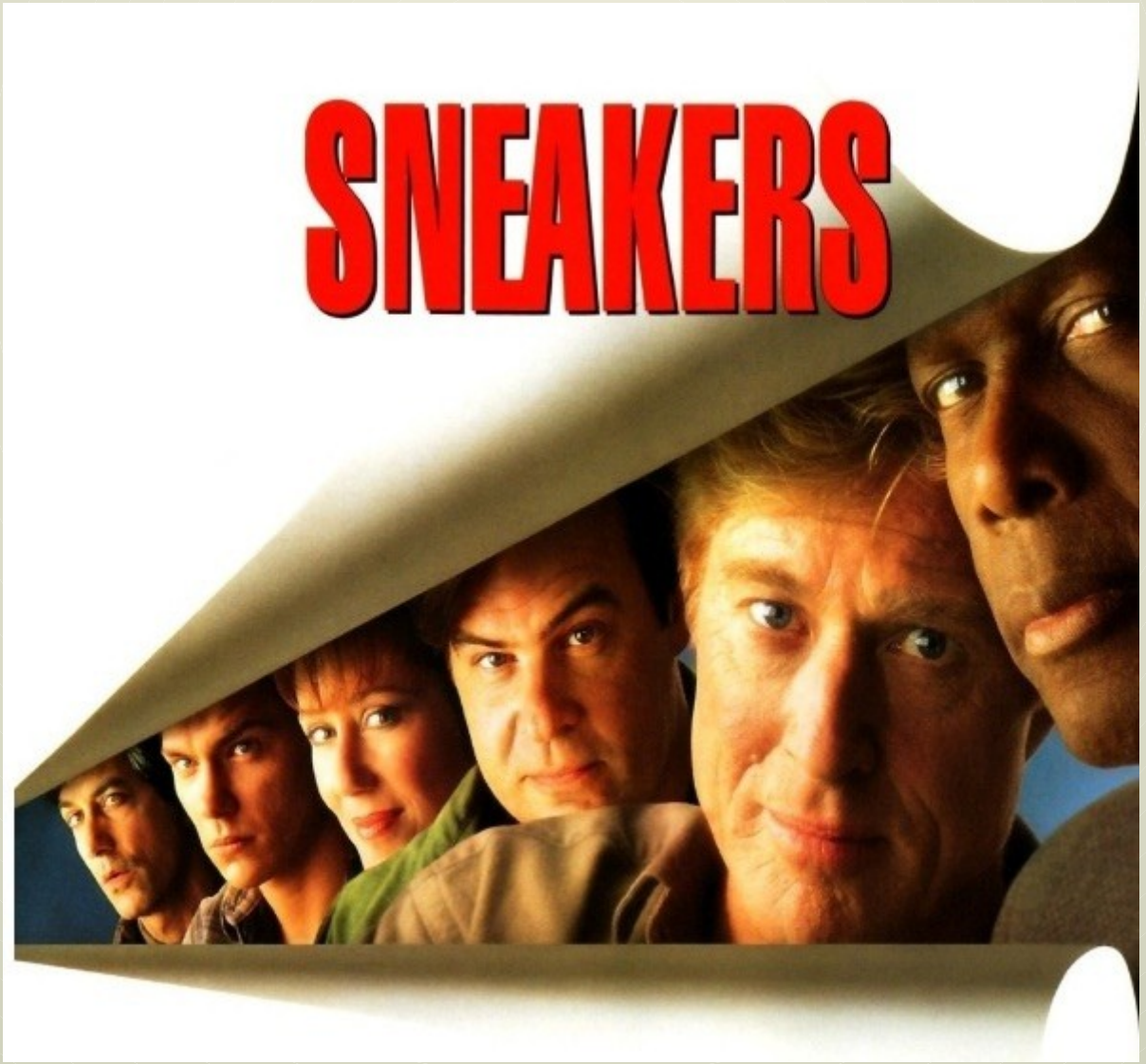
Image by John V Willshire

Automated Cryptanalysis



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

Modern Cryptography



One-Time Pad

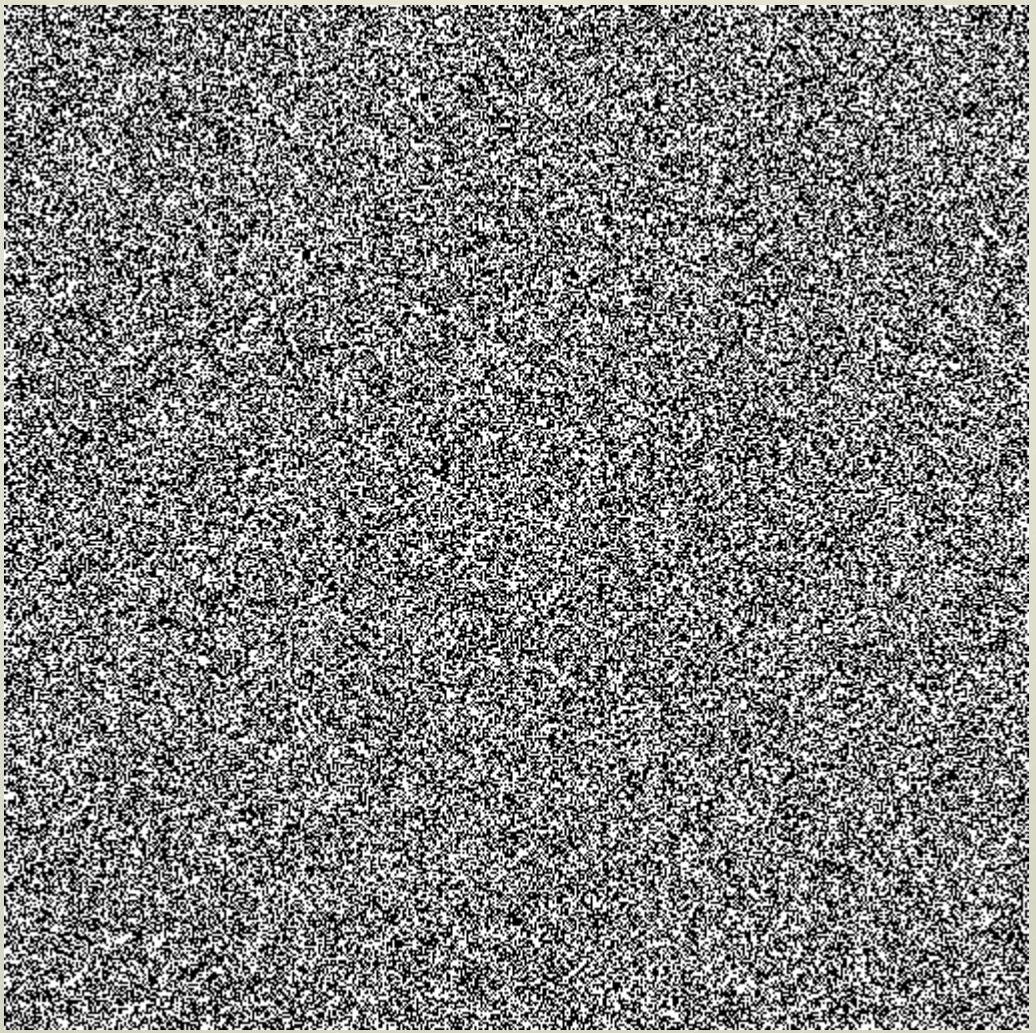


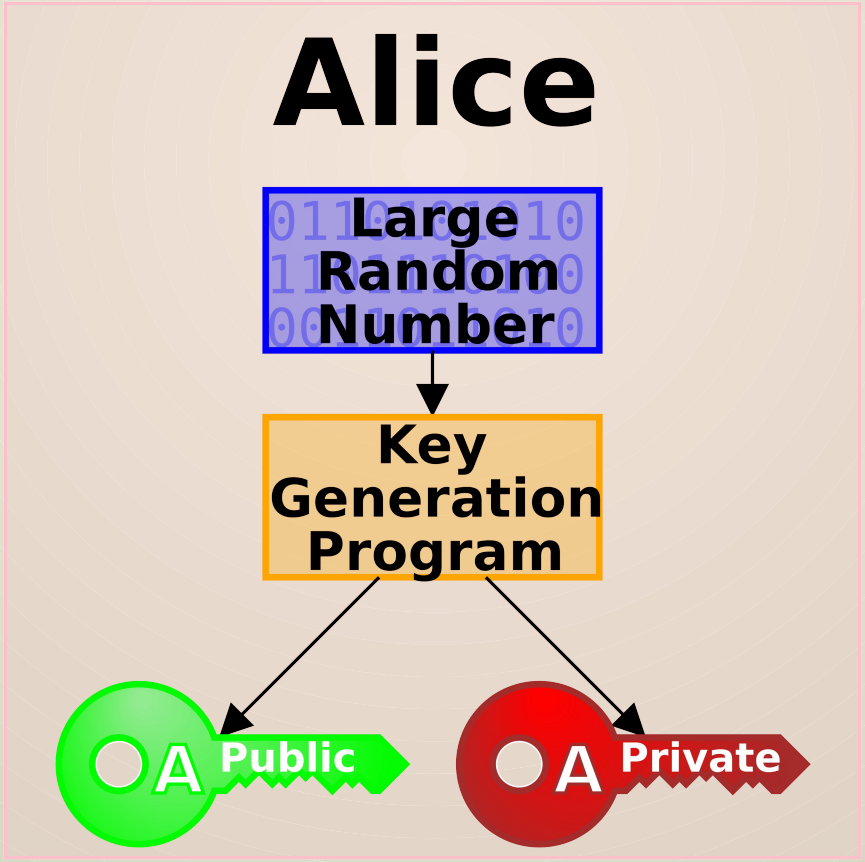
Image by Bo Allen

One-Time Pad Instructions

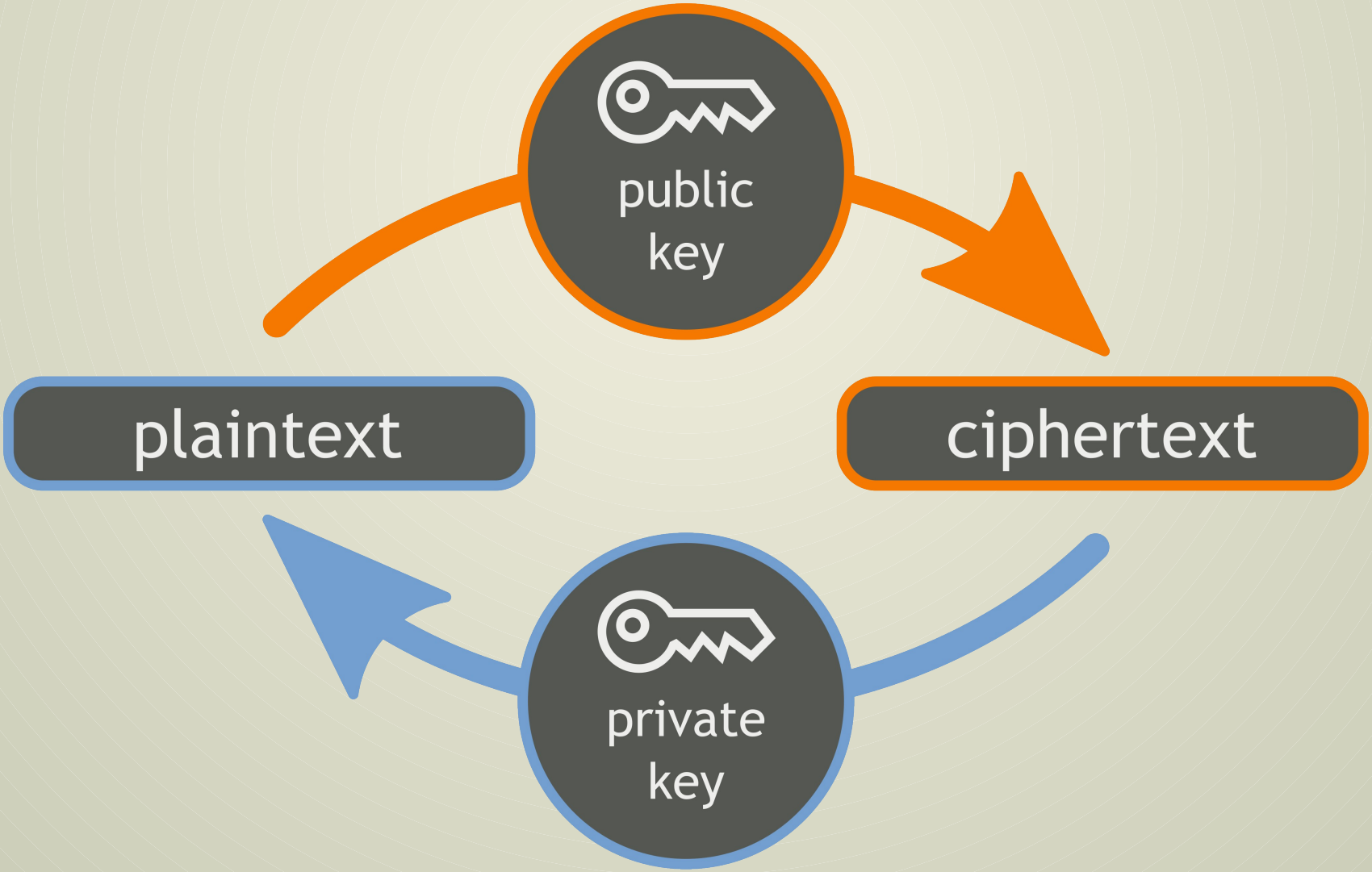
- Generate random numbers for key, *perfectly safely*.
- Exchange key with recipient, *perfectly safely*.
- Encrypt plaintext by addition with key.
- Dispose of key, *perfectly safely*.

Venona Project

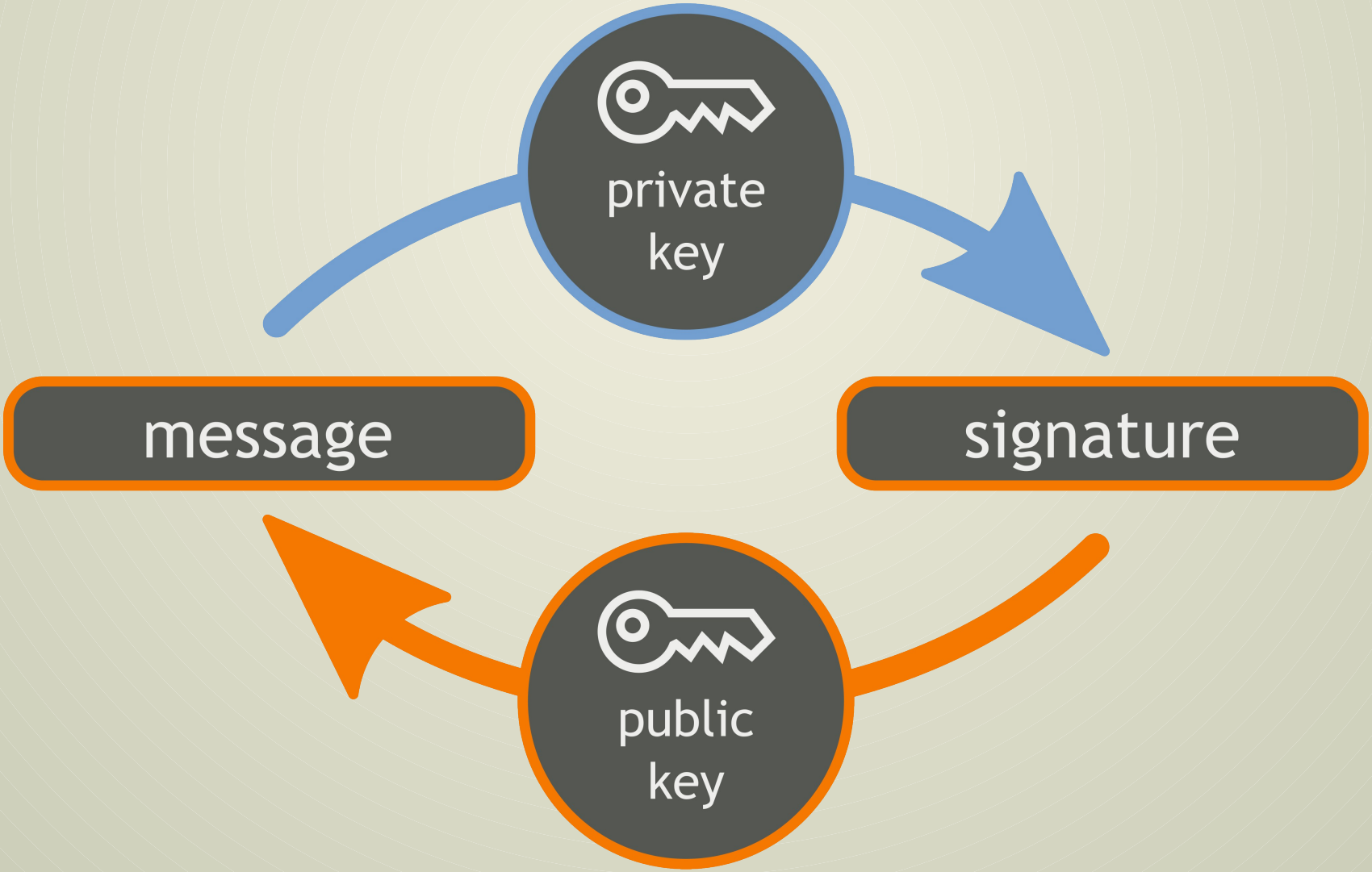
Asymmetric Keys



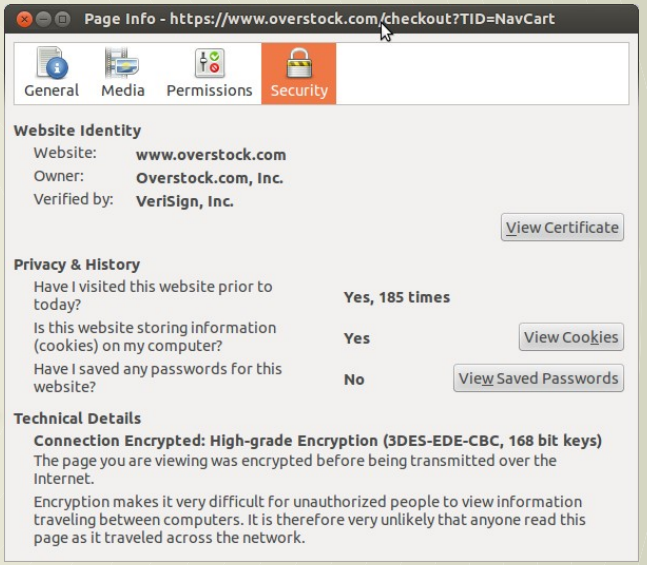
Public-Key Encryption



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: $de \bmod \operatorname{lcm}(p-1, q-1) = 1$

$$\therefore 3d \bmod 8840 = 1$$

$$\therefore d = 2947$$

- 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 = “Hi” ≡ [72, 105] ≡ 9321
- Encrypt: $c = m^e \bmod n$

  $= 9321^3 \bmod 17947$

  $= 9441$
- Decrypt: $m = c^d \bmod n$

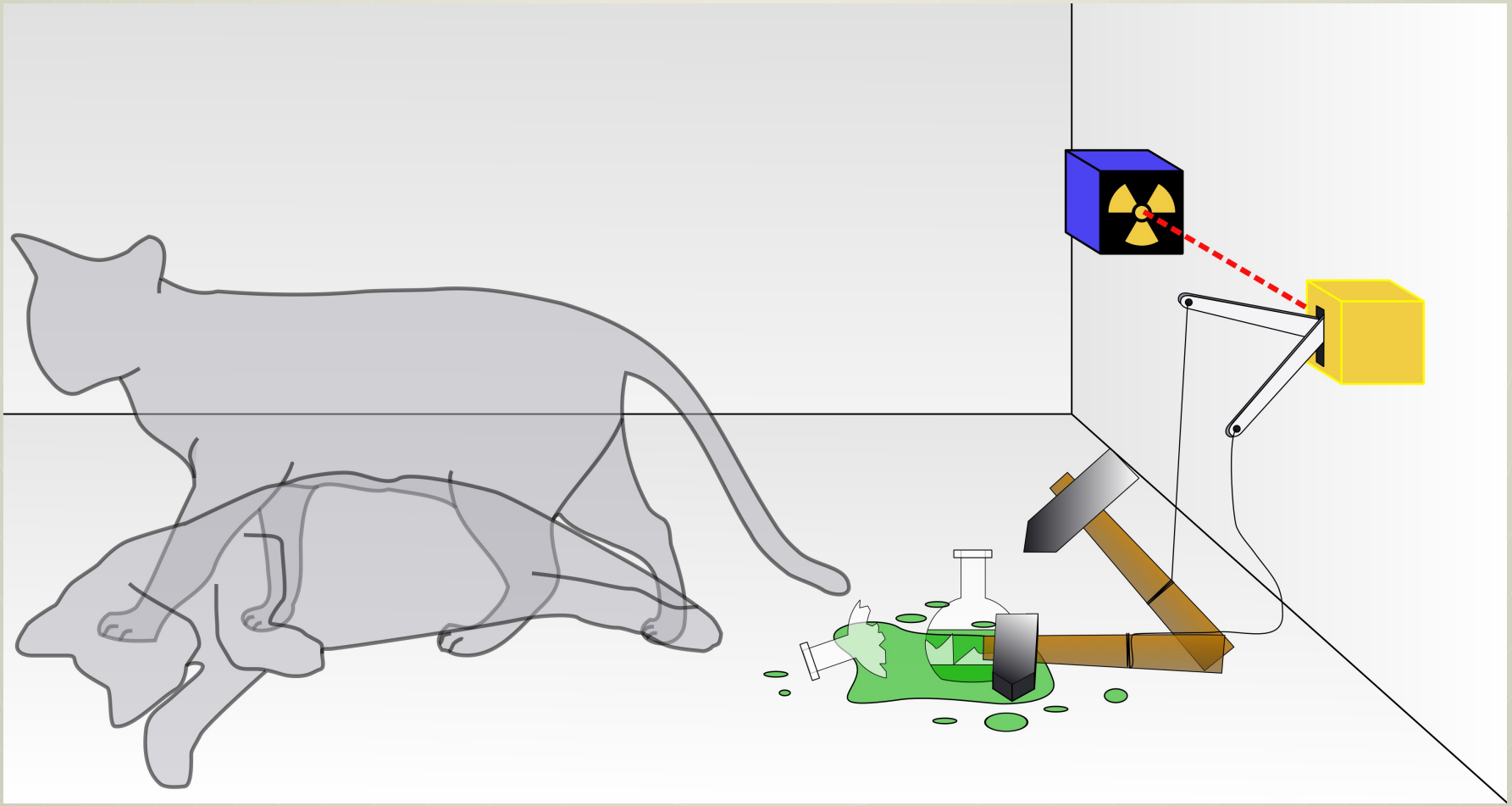
  $= 9441^{2947} \bmod 17947$

  $= 9321$

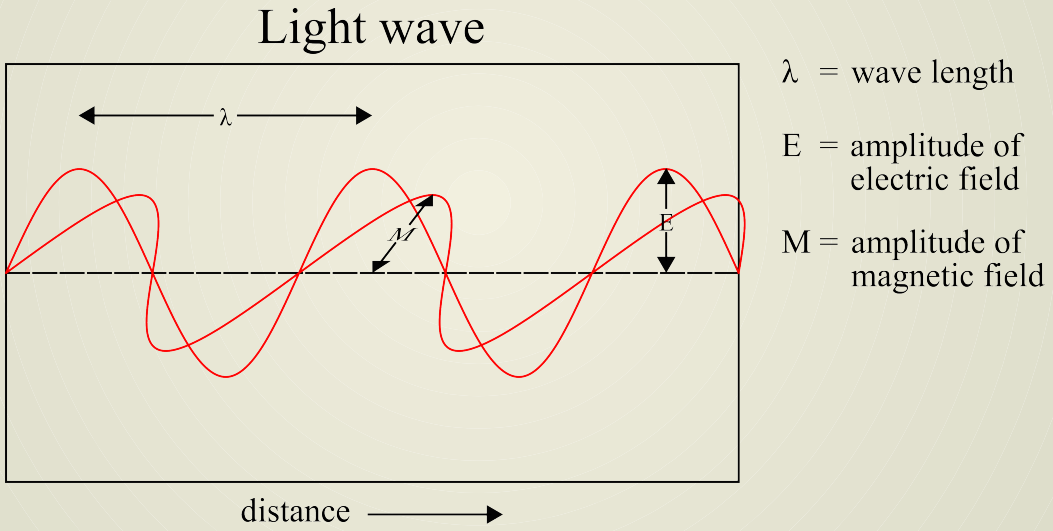
Public-Key Reliability

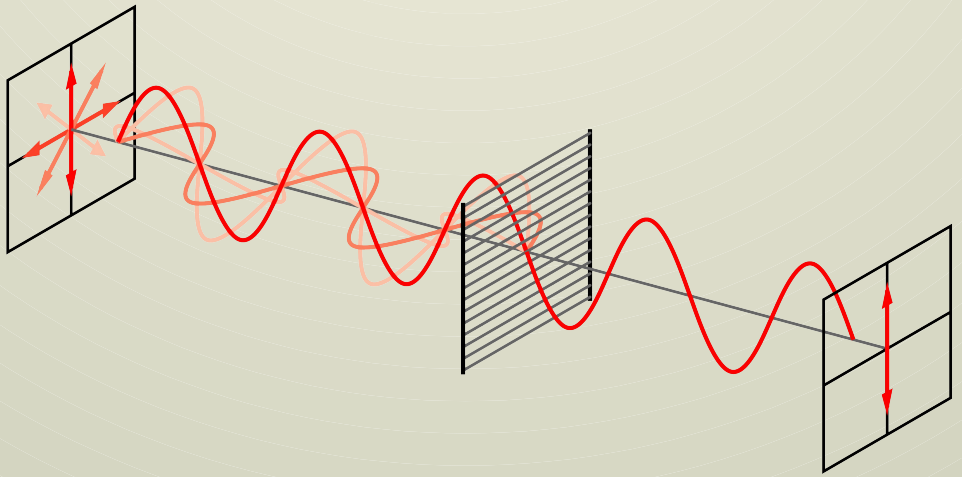
- Using the key incorrectly voids the warranty.
- Don't use the same key pair for both encryption and signing, unless your system gives you permission.
- The underlying factoring problem may be solvable.
- The TWINKLE device can brute-force keys.

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

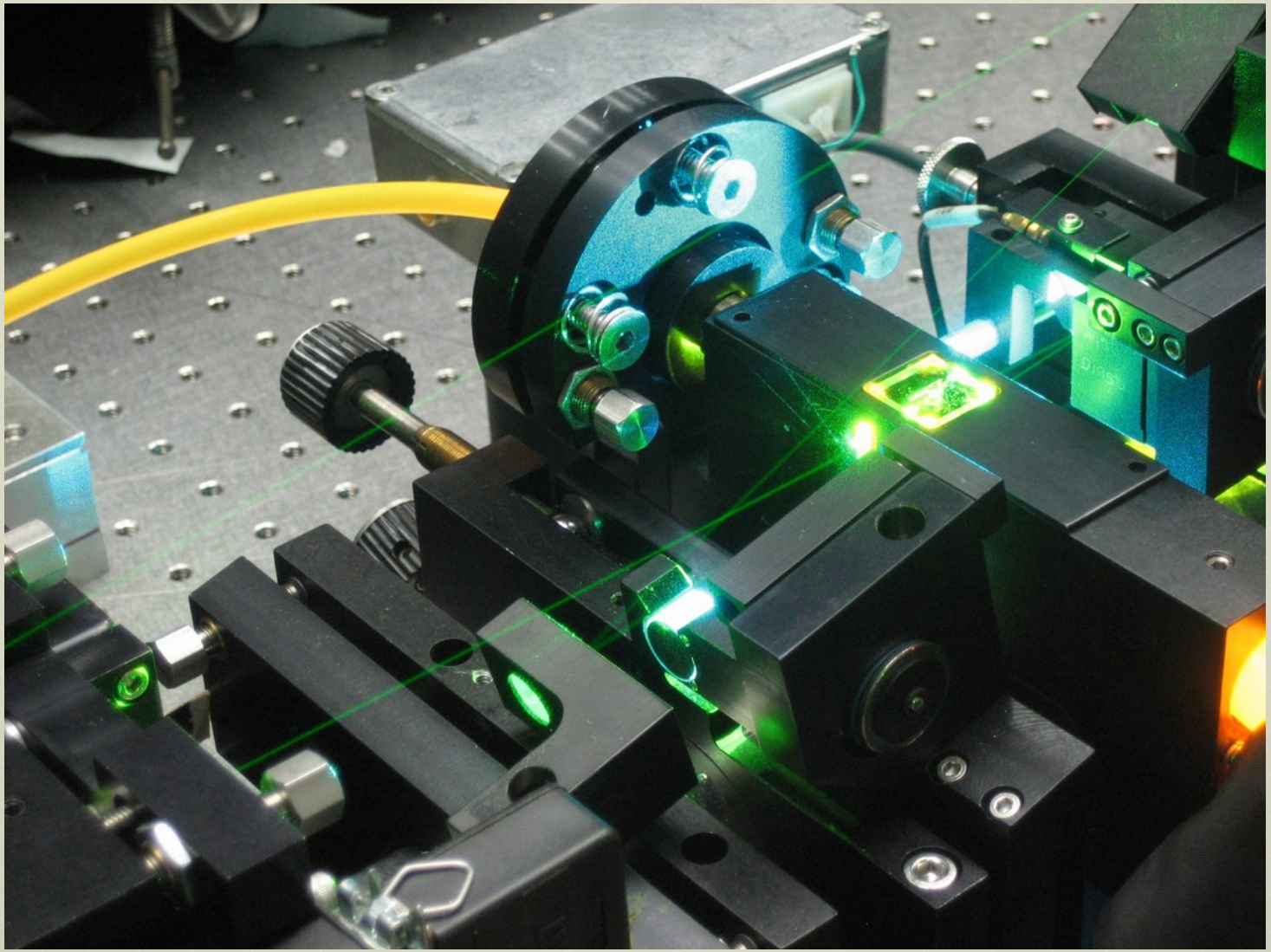


Image by “fatllama” on Flickr

Side Channel Attacks

Cryptographic proofs assume knowledge of all attack vectors.

Successful attackers will break the rules.

Acoustic Cryptanalysis

Capacitor Hum

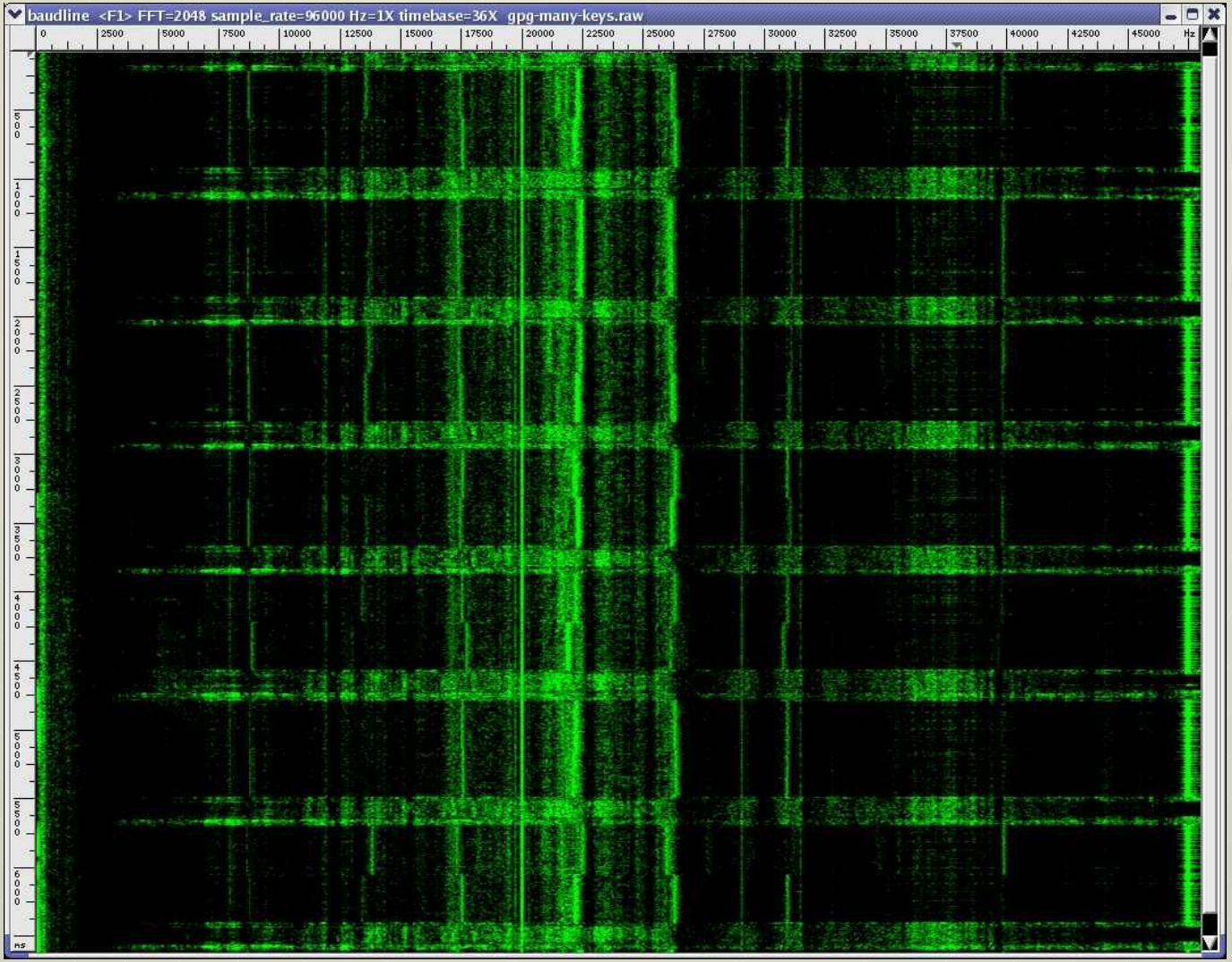


Image by Adi Shamir and Eran Tromer

Suitcase-Full-of-Money Attack

Image by “401(K) 2012” on Flickr

Rubber-Hose Attack

Image by Sam Ley “phidauex” on Flickr

Social Engineering

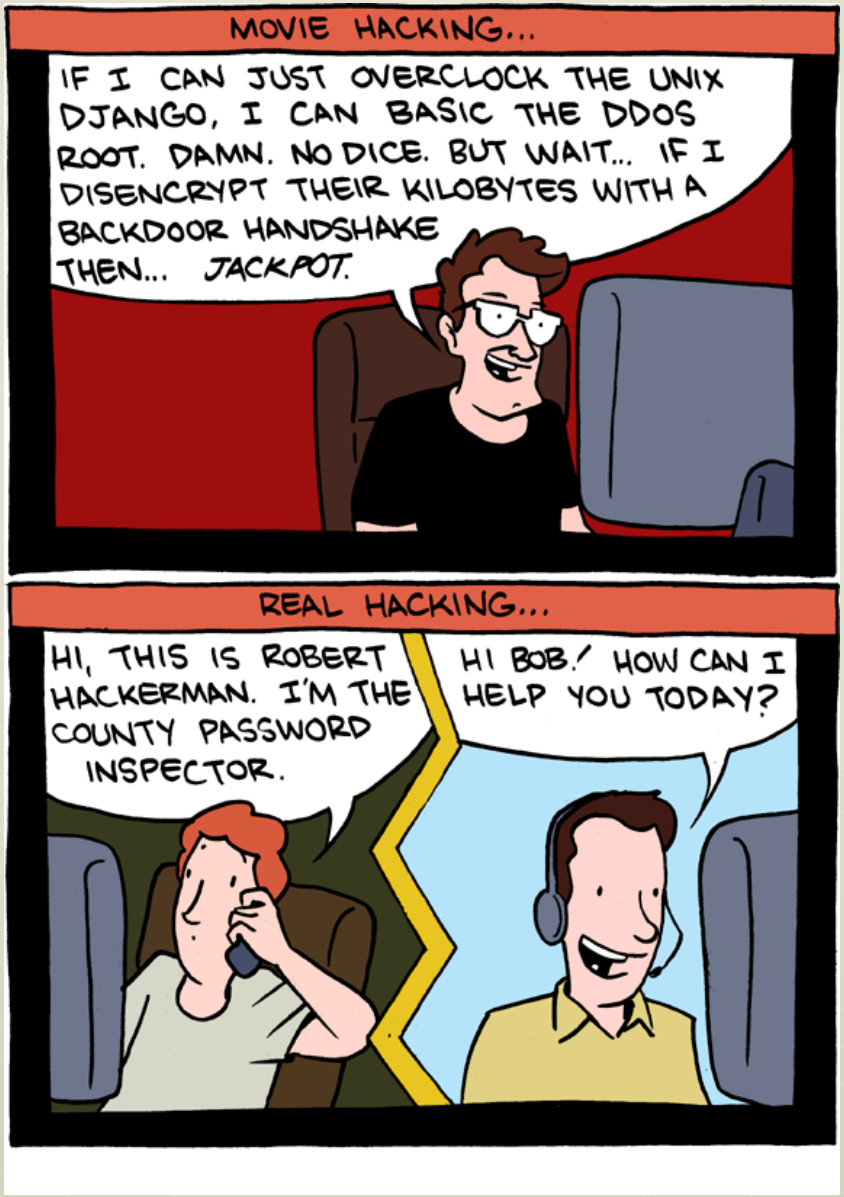


Image from http://www.smbc-comics.com/index.php?db=comics&id=2526

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.