

# Introduction to Applied Cryptography

Nick Hoffman

cinci  
2600

~# whoami

Winner of the 2006 Cryptologia national undergraduate research award.

Winner of the Greaves Scholarship award for research in HFE Cryptosystems.

Published in Cryptologia.

Recently joined the Metasploit project.

Convinced that Linux will take over the desktop

cinci

2600

# Goals:

Explain the principles of cryptography.

Programming? Do you need to understand it?

Why is it important?

# Cryptology vs Cryptography vs Cryptanalysis

Cryptography is code making.

Cryptanalysis is code breaking.

Cryptanalysis + Cryptography = Cryptology

# Principles of Cryptography



Auguste Kerckhoffs

The system must be practically, if not  
mathematically, indecipherable;

cinci  
2600

It must not be required to be secret, and  
it must be able to fall into the hands of  
the enemy without inconvenience;

Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;

It must be applicable to telegraphic  
correspondence;

cinci  
2600

It must be portable, and its usage and function must not require the concurrence of several people;

Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

Diffusion means that flipping a bit of plaintext should affect several bits of ciphertext and vice versa. Diffusion is accomplished by substitution.

Confusion means that there should not be a simple relationship between the ciphertext and the key. Confusion is accomplished by permutation (transposition).

# Caeser Cipher

Shift the letters of the alphabet keeping them in order.

**ABCDEFGHIJKLMNOPQRSTUVWXYZ**  
**CDEFGHIJKLMNOPQRSTUVWXYZAB**

Why it is good?

Easy key to remember = Shift of 3

# Caeser Cipher

"Storm the castle on the first"

becomes

"uvqto vjg ecuvng qp vjg hktuv"

Why is it bad?

Easy to break! Small key space = 26

# Random Alphabet

Randomly assign a letter to represent another letter.

**ABCDEFGHIJKLMNOPQRSTUVWXYZ  
QWERTYUIOPASDFGHJKLZXCVBNM**

Why it is good?

Big keyspace = 403291461126605635584000000  
possible combinations.

cinci  
2600

# Random Alphabet

Why is it bad?

It falls to frequency analysis. Patterns of the language still make it through.

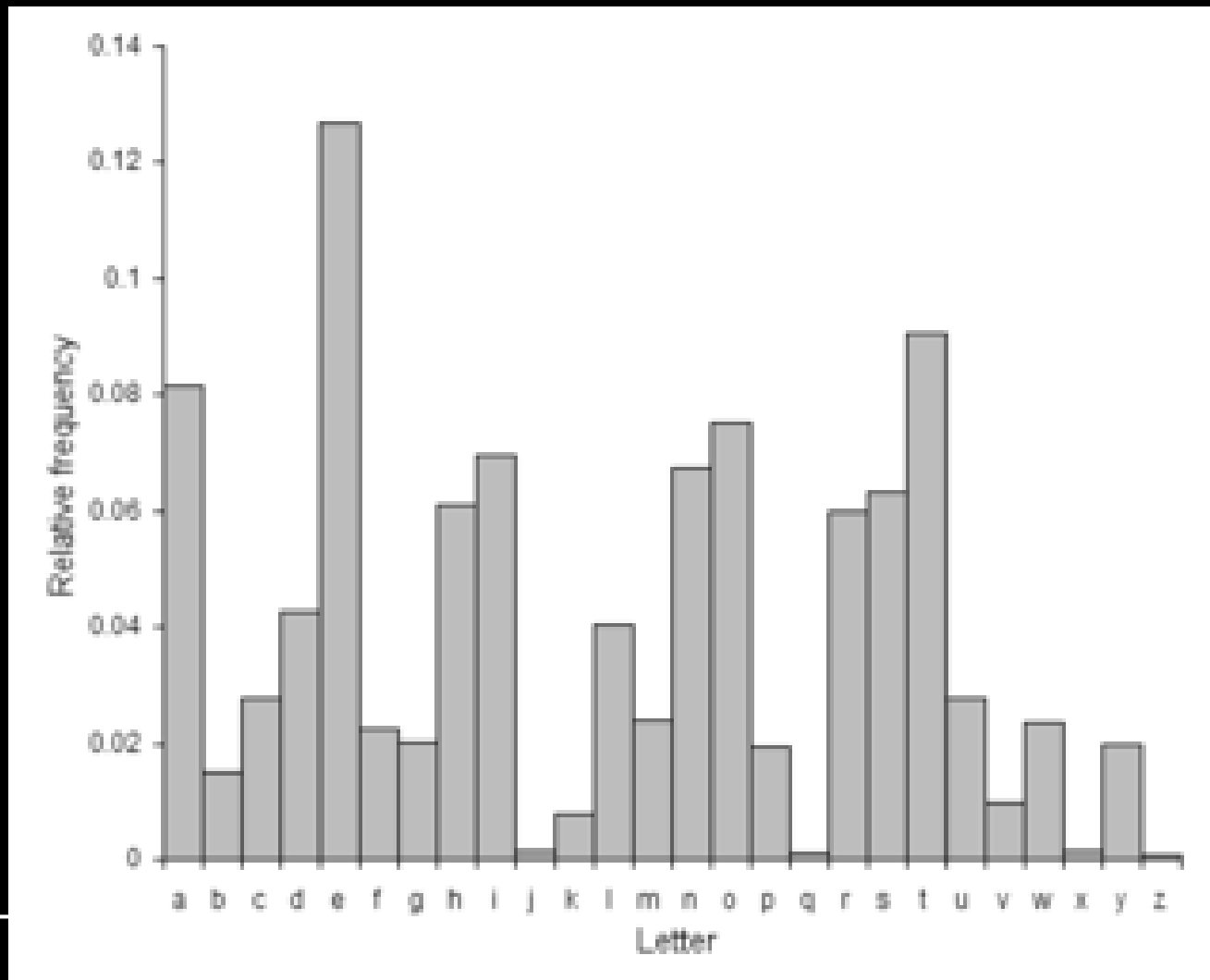
'E' is the most common letter, now it's just going to be something else.

“The” is the most common word. Look for Bi-graphs and tri-graphs.

Not to mention, you're not going to remember that key without writing it down.

# Frequency Analysis

Oh yeah, each language has patterns. Here's English.



cinci  
2600

# Vigenere Cipher



Blaise de Vigenere

# Vigenere 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

cinci  
2600

# Vigenere Cipher

Encrypt each letter using several different alphabets based upon a keyword. This was an early attempt to destroy frequency analysis.

Why it is good?























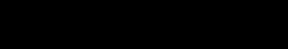

Combines the huge keyspace offered by other ciphers, as well as an easy keyword to remember.

Hurts frequency analysis.

# Vigenerere Cipher

## Example:

When people go on a voyage they often take with them lap-dogs or monkeys as pets to wile away the time. Thus it fell out that a man returning to Athens from the East had a pet Monkey on board with him. As they neared the coast of Attica a great storm burst upon them, and the ship capsized. All on board were thrown into the water, and tried to save themselves by swimming, the Monkey among the rest. A Dolphin saw him, and, supposing him to be a man, took him on his back and began swimming towards the shore. When they got near the Pireus, which is the port of Athens, the Dolphin asked the Monkey if he was an Athenian. The Monkey replied that he was, and added that he came of a very distinguished family. "Then, of course, you know the Pireus," continued the Dolphin. The Monkey thought he was referring to some high official or other, and replied, "Oh, yes, he's a very old friend of mine." At that, detecting his hypocrisy, the Dolphin was so disgusted that he dived below the surface, and the unfortunate Monkey was quickly drowned.

A = 66 =   
B = 8 =   
C = 13 =   
D = 37 =   
E = 100 =   
F = 16 =   
G = 17 =   
H = 69 =   
I = 50 =   
J = 0 =   
K = 13 =   
L = 19 =   
M = 28 =   
N = 56 =   
O = 64 =   
P = 20 =   
Q = 1 =   
R = 36 =   
S = 47 =   
T = 82 =   
U = 18 =   
V = 6 =   
W = 22 =   
X = 0 =   
Y = 21 =   
Z = 1 = 

cinci  
2600

# Vigenere Cipher

Example encrypted with the keyword “dualcore”:

ZBEYR SFTOY GZQBR ZRSAR GHYIB IFEGB KENYW TVVKL HGLLR RFKVI RXQBB IBMAD RSKWW  
IWTNS RADST SGHZQ HNHFU WKJHF LZWHK LDNAX CBIW ORYKB XXRUT SGBJJ UIMEJ SVEVN  
HLFOG IWGOY MSPSQ VOLTR NMWBH TOOJX KYYYG OIIGN HPECR WWIFL VHZGD UGCGO KWWIR  
XDIIW WOPZP HYIPU NOVVV WKCPN CDJMC YDLNZ FREIA CFKVV HNHCO KEMQN OEJSN EWYRL  
PRKVL YDEQG RZHNH POGVP YYSMA GNMPG IYIHY IPINV GMRQR HGEJS IIVNA OQZGL LHSLY  
VZQDH DDWDG SVCNR JWDXR VELOO EXRIK SKAFR KCSMC QBEQX BPIOE WZCMX KBXXR QACFG  
KLHMH ZTSNL HHTSG MXSWH ELTHY ISCRP WGNLL WHTUH YISIR EQTRX KYNDV VVHRF PSKBR  
WNYDE JSDSQ EEJKT YIZUS LPOKL HHILP HYIPI NVGMI ISFIP FHYEW BEHCG RRGUD OGRKL  
DNHPE ODIRZ AGGFP HLMTT PULMV BEOHO DMOST SGBFJ FIUCU SPSXE NZYHY ISCRP WGTSQ  
NIYWS UXKYD ZNDYM QNHPO CEOHS TSQIX LWBEH CGIII YRCKB XXRMO XGVZK KIFQK QZE0I  
RZVVV VDHDC GDCMH XOSAS JLHMA GGFPS OXFCK SEHRZ MTPSR XWBAE FSKIF NIYIV ZWKSP  
ZEFZW BNHPF CCTKC NHCGJ SGCSR WGKIG NHLVV VHLPE ODSCS ZNHPU IIJDW ELPRK LHONQ  
QFKYQ UTPOC EOHSW LUELM FELJF FFAQY D

A = 14 = |||  
B = 22 = |||  
C = 30 = |||  
D = 28 = |||  
E = 37 = |||  
F = 29 = |||  
G = 41 = |||  
H = 52 = |||  
I = 51 = |||  
J = 16 = |||  
K = 35 = |||  
L = 35 = |||  
M = 23 = |||  
N = 34 = |||  
O = 33 = |||  
P = 32 = |||  
Q = 24 = |||  
R = 42 = |||  
S = 48 = |||  
T = 21 = |||  
U = 15 = |||  
V = 33 = |||  
W = 34 = |||  
X = 23 = |||  
Y = 34 = |||  
Z = 25 = |||

# Vigenere Cipher

Ways to break.

Strip alphabets. Throwing every Nth letter into a bucket. If the model matches common letter frequencies, then run Caesar cipher shifts on them.

Why it is bad?

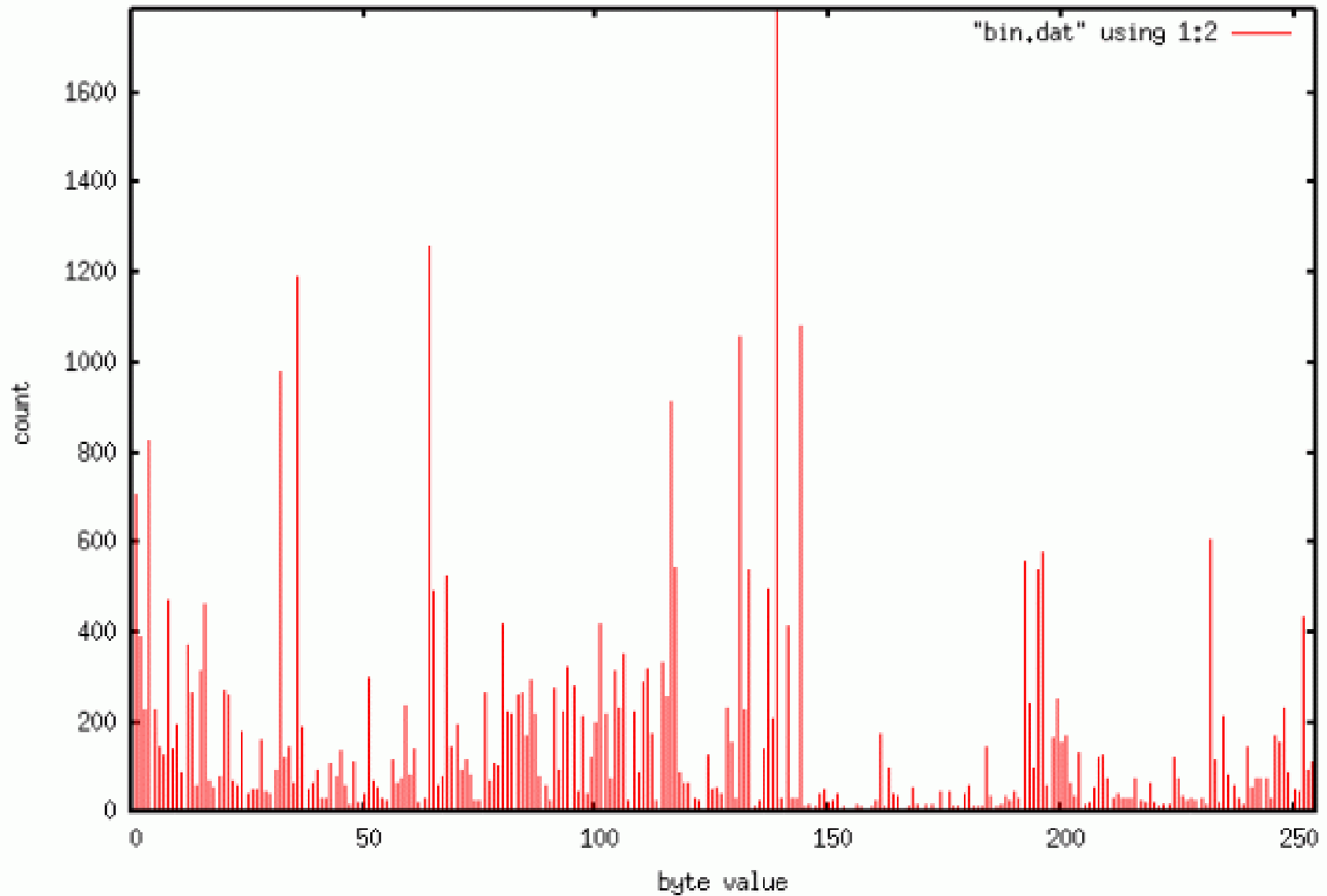
Still falls to frequency analysis although it was designed to be resistant to it.

# Frequency Analysis

Any “ghosts” of the plaintext should be hidden.

Does this apply to modern day text?

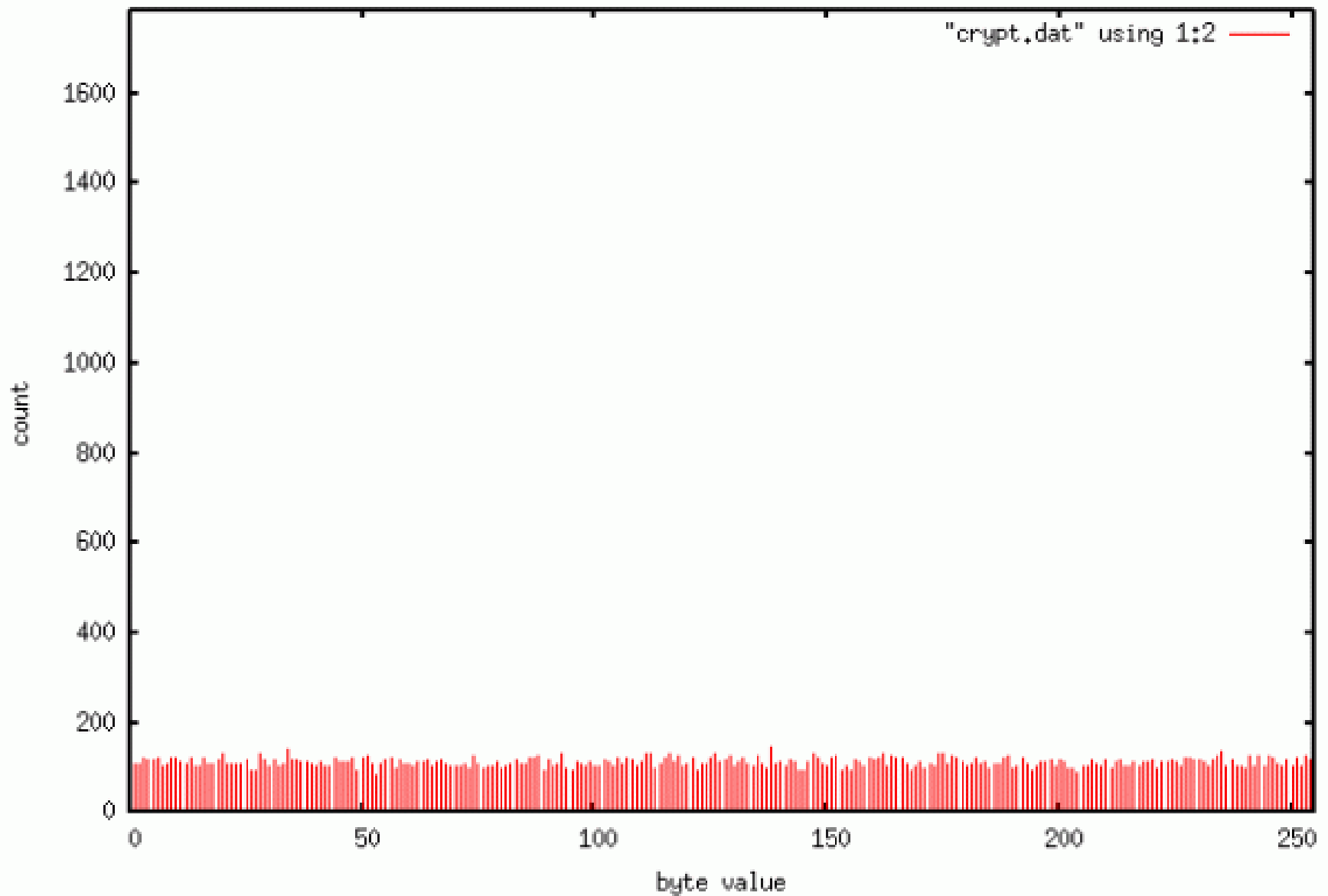
Byte Value Graph of nc.exe



212.597, 1866.67

nci  
2600

Byte Value Graph of nc.exe.gpg



268,265, 1665,52

2600

# One Time Pad

Use a random key encrypting each letter with a different alphabet.

Without a key, this cannot be solved.

Why it is good?

Can't break it! - Wait? Isn't that a bad thing?

# More Than One Letter?

Hill Cipher – Encrypt by multiplying against a matrix

Playfair Cipher – Used to encrypt 2 letters at time. Using transposition.

# A Call for Change

These are all nice, but aren't they just games?

Need something with a little more “backbone”.

Mathematics anyone?

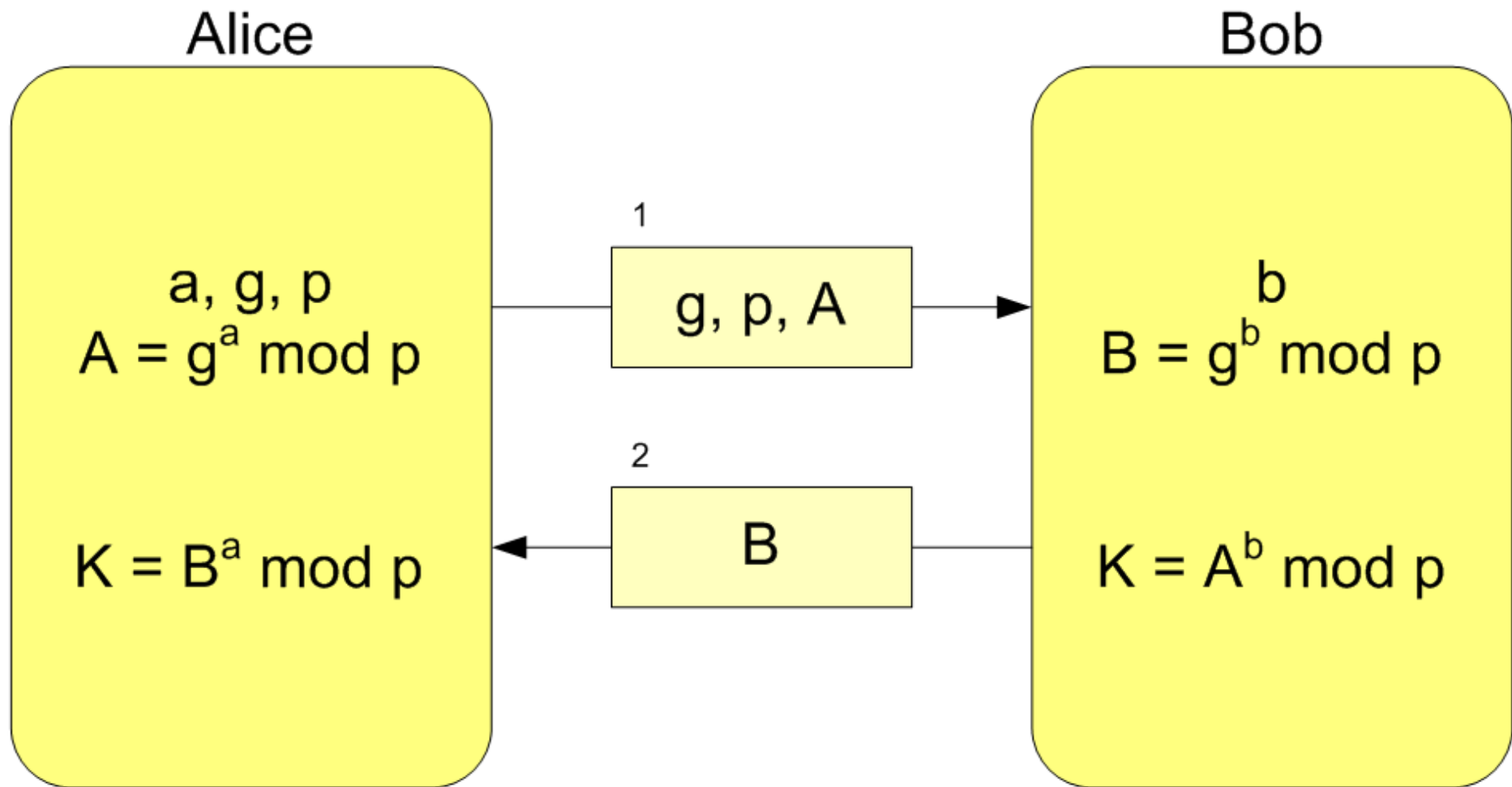
# Mathematics

In general, there are some problems that are difficult to solve.

NP-complete, NP-Hard, factoring problems, etc...

Can these be used to our advantage?

# Diffie-Hellman



$$K = A^b \text{ mod } p = (g^a \text{ mod } p)^b \text{ mod } p = g^{ab} \text{ mod } p = (g^b \text{ mod } p)^a \text{ mod } p = B^a \text{ mod } p$$

# RSA

Relies on numbers being difficult to factor and easy to multiply.

Simple number theory: If  $N$  is prime and  $P$  is prime then the product of  $N$  and  $P$  is only divisible by those two factors.

Example:  $5 * 13 = 65$

# RSA

Still not convinced?

Well, ok.

DEMO

# El Gamel

Relies on the discrete log problem.

Let's take a look.

Vocabulary for this chapter: Primitive root

# Discrete Logarithm

Prime numbers are guaranteed to have at least one primitive root.

A primitive root is when you take a prime number let's say  $Q$ . You take a root, let's say  $A$  and you take all the exponents from 1 through  $Q-1$  ( $N$ ).

You then test for all values in the form of :

$$A^N \bmod Q$$

# What is he talking about?

Let's take

Prime = 7

A = 3

$$3^1 \bmod 7 = 3$$

$$3^2 \bmod 7 = 2$$

$$3^3 \bmod 7 = 6$$

$$3^4 \bmod 7 = 4$$

$$3^5 \bmod 7 = 5$$

$$3^6 \bmod 7 = 1$$

Let's take

Prime = 7

A = 4

$$4^1 \bmod 7 = 4$$

$$4^2 \bmod 7 = 2$$

$$4^3 \bmod 7 = 1$$

$$4^4 \bmod 7 = 4$$

$$4^5 \bmod 7 = 2$$

$$4^6 \bmod 7 = 1$$

Demo

cinci  
2600

# I See a Problem

What if.....

Someone solves the number factoring problem tomorrow?

You wake up in the morning and find the solution to the discrete log problem?

# Nick, are you trying to tell me....?

...that these crypto systems rely on a single number theory problem that is difficult to solve?

...that every time the key for one of these things (512, 1024, 2048, etc.....) is essentially just patchwork and not a solution to the bigger issue in sight? Wait, I think I know something that would be a potential problem.....

cinci  
2600

# Quantum Computer

Shor's Algorithm – Goodbye RSA, EL GAMEL.

Factoring numbers is no longer an issue. At all.

Worry about it?

IBM claims to have factored 15 with a “quantum computer” using an implementation of Shor's algorithm.

# Hmmm, well crap.

Don't worry too too much about quantum computers yet. Let's think about this a little.

Mathematics will not have every single problem solved with a quantum computer. There are still “quantum resistant” algorithms out there.

Not to mention the ever popular quantum crypto.

cinci  
2600

# NTRU

The name Ntru is short for N-th degree truncated polynomial ring.

# Hidden Field Equations

HFE looks forward to a post-quantum world where the number theoretic public key cryptosystems – RSA, ElGamal, and ECC – are no longer secure.

$$\tilde{F}(X) = \sum_{i=0}^{r-1} \sum_{j=1}^i a_{i,j} X^{q^i + q^j} + \sum_{i=0}^{r-1} b_i X^{q^i} + c \in K[X]$$

# How Injective are Hidden Field Equations?

Similar to the discrete log, there are equations which are not perfectly injective.

Is this an issue?

# You Forgot About Block Ciphers!

Block Ciphers such as AES, DES, IDEA and 3DES are also currently being used.

Block ciphers are fast. Usually computing trivial things: XOR, +, or a lookup table.

They can be put on a chip. Minimal software necessary.

# DES

1977 the National Bureau of Standards (now NIST) released DES based upon IBM's Lucifer algorithm.

64 bit key (8 parity check) so in all reality a 56 bit key.

Lucifer had a 64 bit or 128 bit key, why weaken DES? Conspiracy theorists, go nuts.

# 3DES

1998 the EFF constructed hardware that would do an exhaustive search of DES keys. As a result DES was broken in 56 hours. DES was doomed.

Since DES is not a group, re-encryption does enhance security.

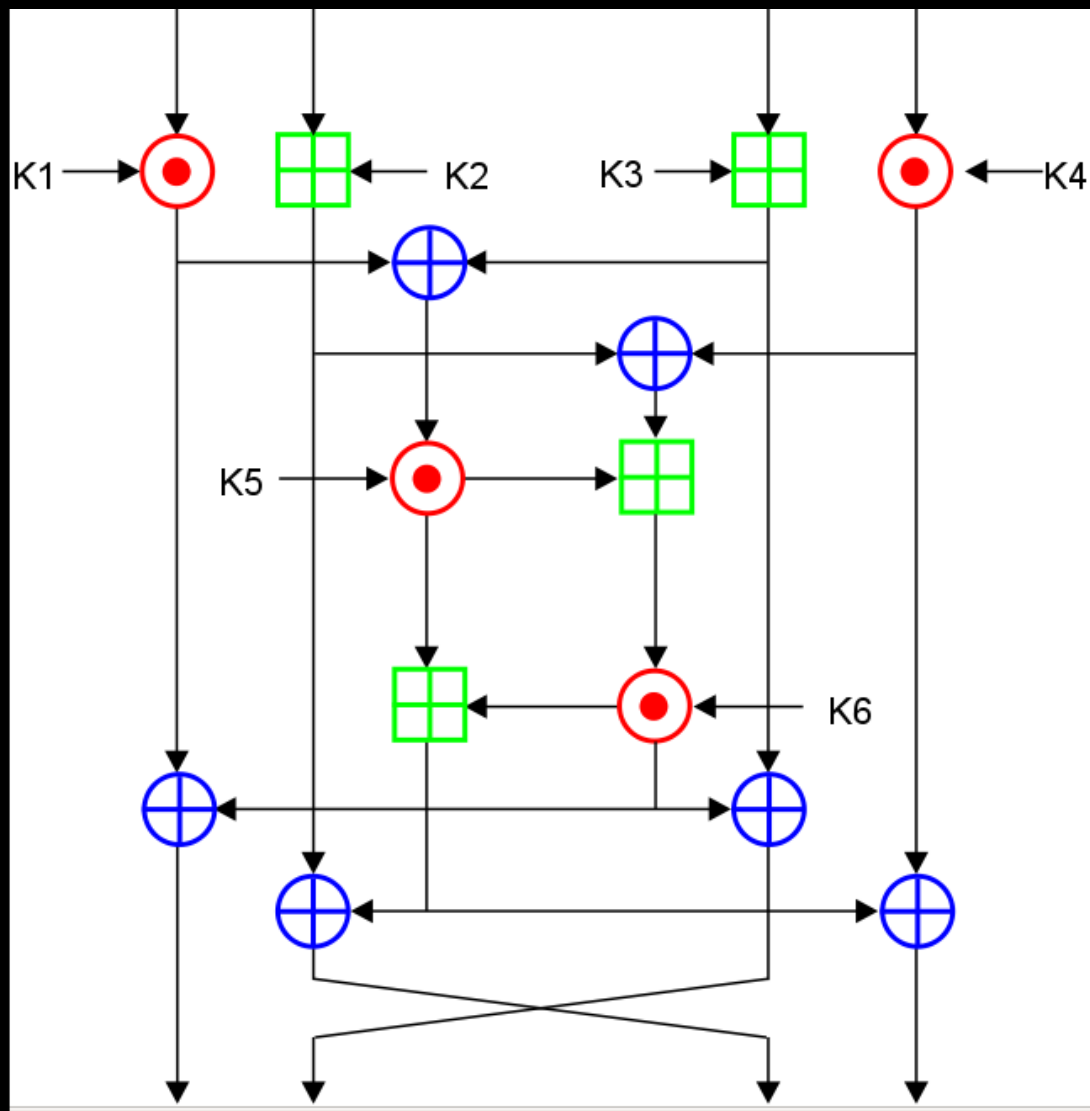
# IDEA

Developed in 1991, the International Data Encryption Algorithm was hyped by even Schneier.

It never did replace DES but was used in PGP. It was copyrighted (still is) and that held it back.

IDEA is somewhat unique in how it handles keys....

# IDEA



# AES

AES is a substitution-permutation network. (SP network). In a round S-boxes (diffusion) and P-boxes (confusion) transform the blocks of plaintext.

Attacks on AES?

XSL - Solving multivariate quadratic equations

Nick, I'm a programmer.

How the hell does this all apply to me?

I lost you back on primitive root.

cinci  
2600

# The Question Remains

What do we do now?

Look somewhere for more 'elegant'  
mathematics?

Rely on quantum crypto?