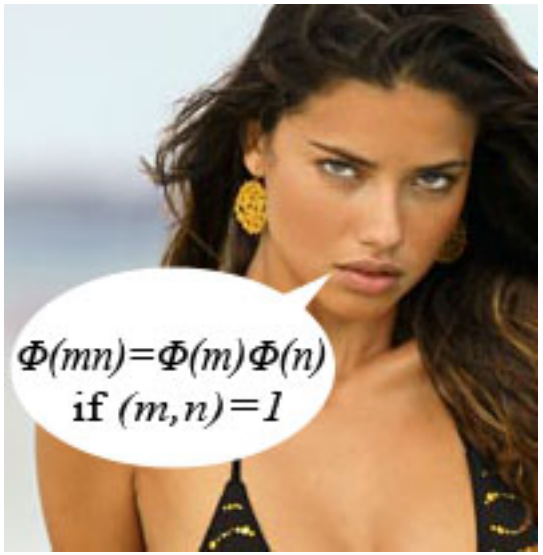
The
Melbourne
University
Mathematics and Statistics
Society

presents:

Victoria's Secrets



Daniel Yeow

March 12 2006

The Science of Secrecy

Steganography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to **cryptography**, where the existence of the message itself is not disguised, but the content is obscured

Some Definitions

- **Cryptography**, literally "secret writing", is the art and science of designing ciphers

- **Cryptanalysis** is the art and science of breaking ciphers

- **Cryptology**, literally "science of secrecy", encompasses both aspects

Code or Cipher?

- A **code** – A code is a very particular type of secret communication. In a code, a word or a phrase is replaced with a word, a number or a symbol. For example "nasty vietnamese communist soldiers" might be replaced by the code word "charlie".

- A **cipher** – In a cipher, individual letters are replaced rather than whole words. For example, the above phrase would be replaced with "eidmw qudkbrexws qopdkzlrt soudyebq".

we will primarily be talking about ciphers

Unbreakable Ciphers?

- Controlling message length may render a cipher unbreakable – *unicity distance*

Some Cryptographic Primitives

Definition A *secret key cipher* is a *5-tuple* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ where the following contitions hold:

- $\mathcal{P}$ is a finite set of possible **plaintexts**
- $\mathcal{C}$ is a finite set of possible **ciphertexts**
- $\mathcal{K}$ is a finite set of possible keys, also called the **keyspace**
- For each K $\in \mathcal{K}$, there is an encryption rule $e_K \in \mathcal{E}$ and a corresponding decryption rule $d_K \in \mathcal{D}$. Each $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ are functions such that

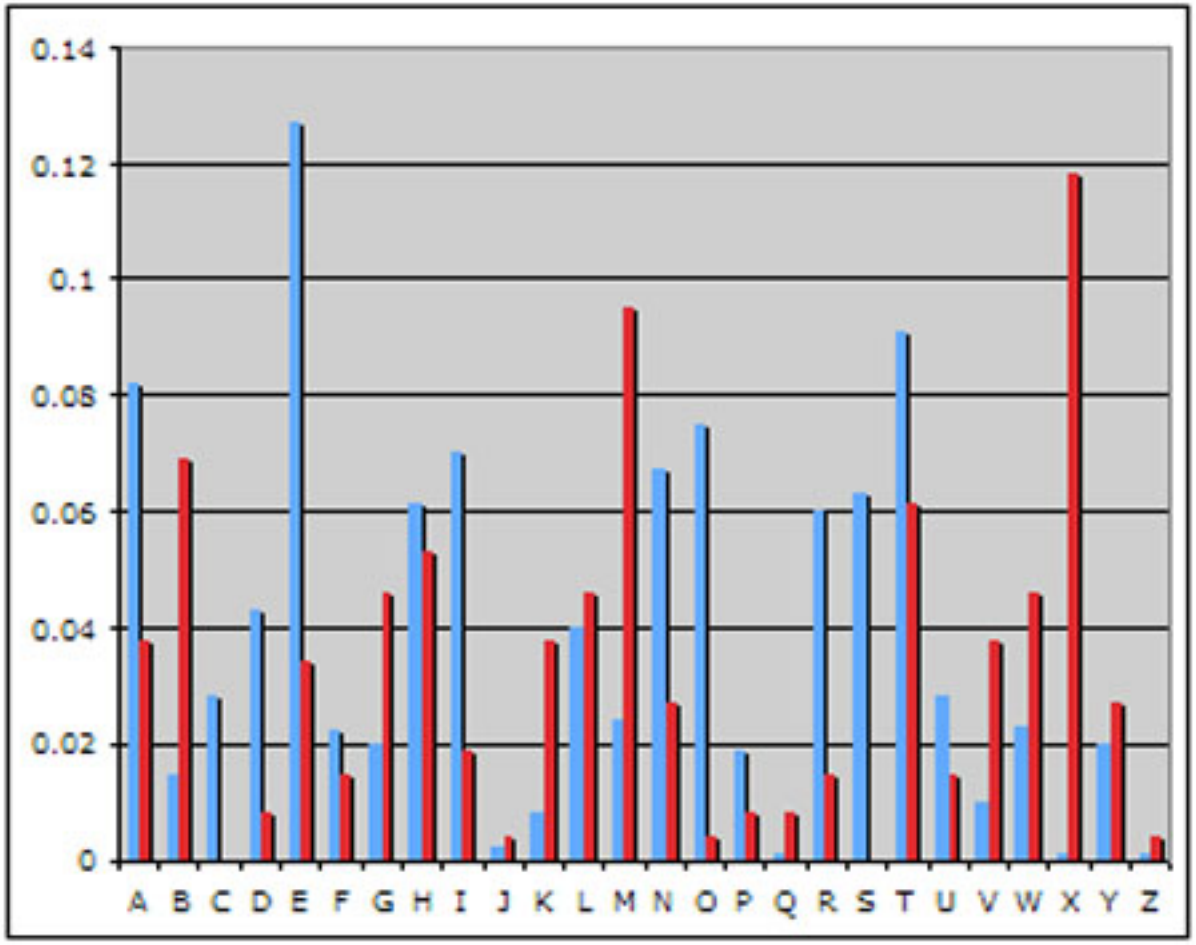
$$d_K(e_K(x)) = x, \qquad \forall x \in \mathcal{P}.$$

Kerchoff's Principle states that the design of the cipher is not kept secret. To sum up, we avoid "security through obscurity". All security resides in the secret key.

Lets try one

”par whgm rhn wxvhwx lhfxmabgz t ebmmex fhkx wbyybvnem max vtxltk labym bl hgx hy max xtlbxk xqtfiexl hy t fhghteiatuxmbv lnulmbm-nmbhg vbiaxk bm bl onegxktuex mh exmmxk ykxjnxgvr tmmtvdl tgw phkwl ebdx max tgw t vtg ux bwxgmbybxw tgw nlxwmh wxvkrim max vbiaxkmxqm”

Letter Frequency for the Ciphertext



In the 9th century, the Arabs were the first to record a method for breaking the monoalphabetic substitution cipher. They did it by using letter-frequency analysis.

How can we combat letter frequency analysis?

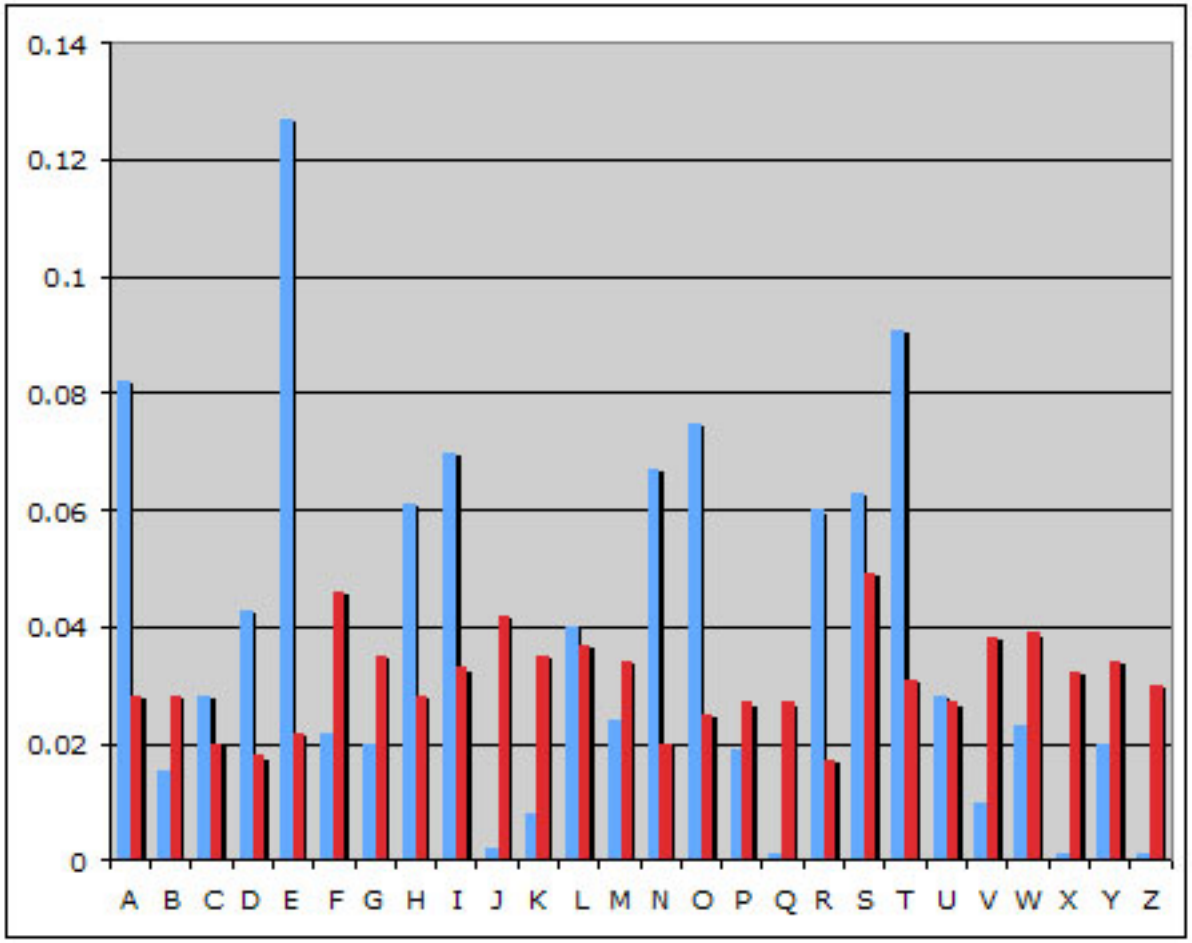
One way is to use more than one alphabet, so instead of a *mono*alphabetic substitution cipher, we have a *poly*alphabetic substitution cipher. The *Vigenère cipher* was one of the first ciphers to do this. (Aside: Mr Vigenère didn't actually invent the Vigenère cipher, he invetend one of the first forms of *autokey cipher*, a slightly stronger form of polyalphabetic substitution cipher). These ciphers were considered to be unbreakable until at least the late 19th century. The process is quite tricky, and without modern computers, very time-consuming.

Let's try one of them

"viiyj ybw rgxfqlsl bx yzg waflkpr kgt xoj ypvk zce wfkufh fjqvrk ljbx yzg gvql gvvr qmh wwisia zce ntl bahd coh msf nvnfge amw xmsi dvwo zqswlx jf dfk xsyyz b amgwteui rpyui up hqd ull utbgrx jbh lsviiyjv us yzg jyfq bps ljf awage hsv osajv smkjju jyte ull kvbxptfu rlfj brk xcs ofv nyzywtfh fl ull zqnizywce vawtomnml gsy ljf izkjniu dqwi mste ynvkok bzgsi yzg apqv cyzm jpvzjk bvl spe amw txvhc-isyxw trbkxu xoj dbxaqw xmam ffpplzv xojjg ahx jbvynkqo, bzq qhiw imz hkmi bzgo wfjfpr bgp xoj evt yzg ssi obr bavi onk iepw ct dmavf hx uosd twu mjo dsbqv smkj dfwpiw imt ojfr mau fstgf ahx hbmyqq vt mw xsbqv hs bzgsicjj isyxw brk eco jtmne nt coh hdcogf gh xoj qwiykdqx jfeg hvbf us qwpe h zcoh sg ciaywt lvwkgneu wxfv mwne amw sipsk gsy fgwiy zqswl uqvpk ljssd zkn dmanf amw tekidg-kpwljt dtmne zyspe oj nfeysl us waff dmanf kwgxjrn gp xoj rmepsk brk gpf dfk ullww, e

xltjtsnfi su s tqhqd brk ogfhf tgbwa zg ahx upqlyzkok qamf h jcdiotjuf bsvgswpewf apyz b atmei vk vjqvw rprf ljsil hcsxz ljpvvzyjcvli cu sjsuu hsv tyjm ct hww cc rgwoxhnf isyxwofr ujkaik zg ahx jbvk spe atmii hsv xmyd - nbxl ull kqsx yzcu dtf'u zfq eml ljfvl oct jtmtbkl ap lpx svmjp knthyagox yjgbh fff ll tqsi yzg fhiyg sm ycniujku mu zkt xzael hsv gmlwq fcl spe amw qvvzv brk dqgxf ucsvpfyg sm zkt ojsf'

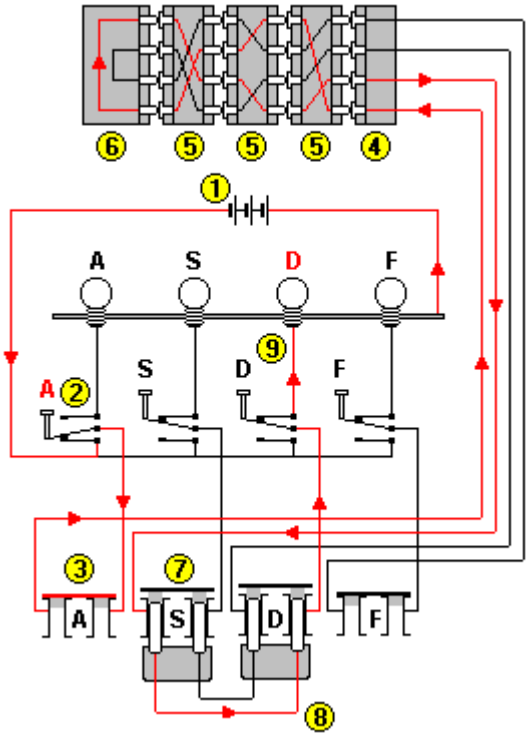
Letter frequency for that one



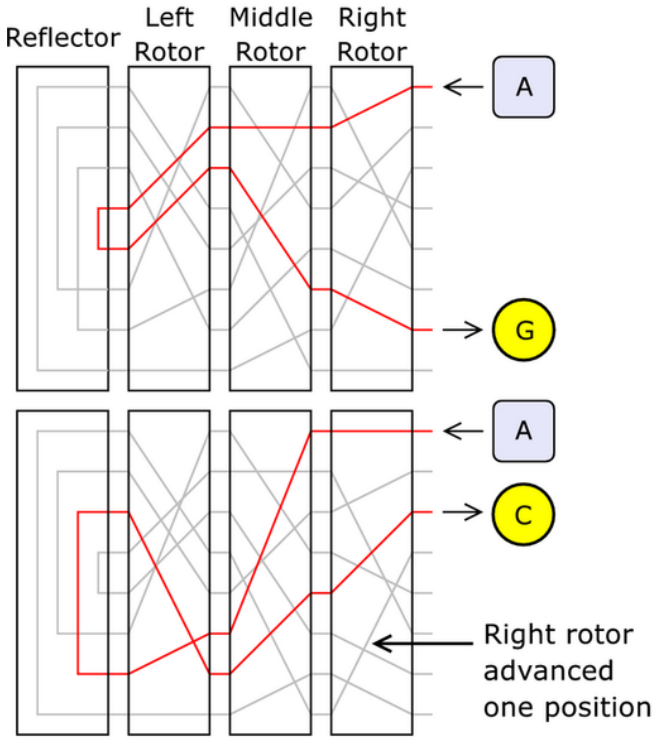
A useful square...

	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

Enigma



How it works



As letters are typed into the machine, the rotors turn, permuting the combinations. In addition, there is a plugboard and scrambler.

How it was cracked

Alan Turing played a pivotal role in the cracking of the Enigma cipher.

We won!

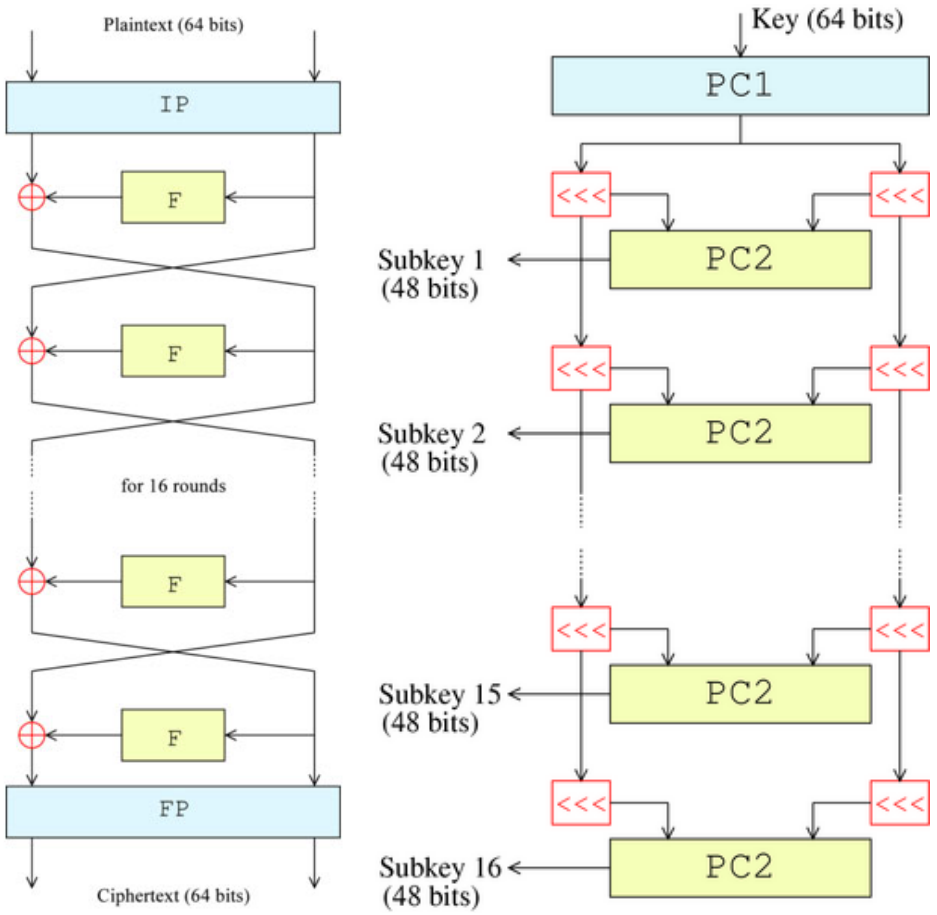
So, you say... surely we can produce stronger ciphers with all of our modern technology?

we can

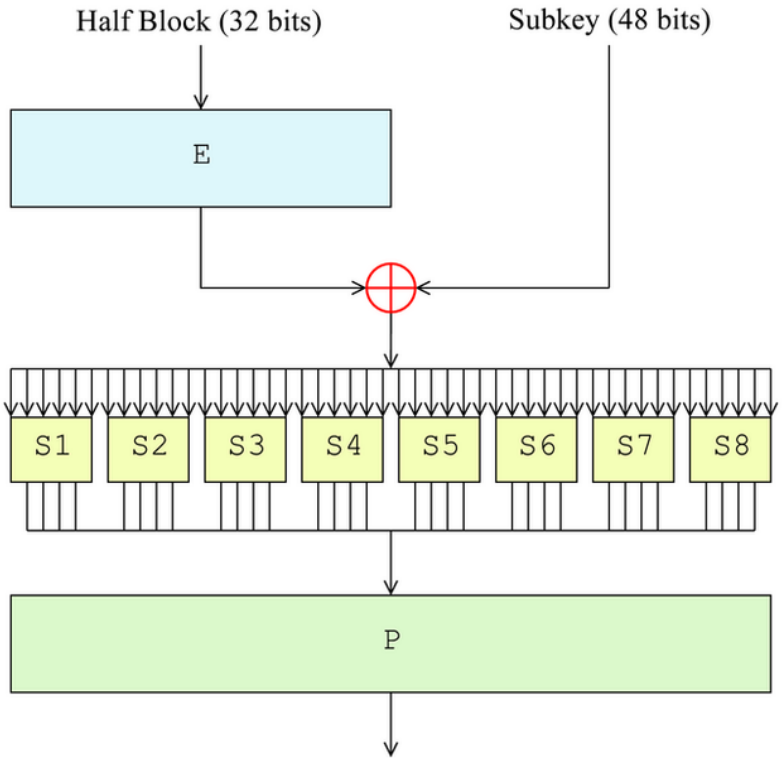
I will now show you the nuts and bolts of a modern encryption system.

The **Data Encryption Standard (DES)** is a cipher selected as an official information procession standard in the United States in 1976. It was developed by IBM for the US government under great controversy including suspicions of a National Security Agency (NSA) back door. It is a **Fiestel network** whose security depends primarily on the design of **substitution boxes (s-boxes)**. Although considered insecure given the advances in computing power since 1976, it still has many practical applications (like triple-DES). In recent years it has been superseded by the **Advanced Encryption Standard (AES)**.

How it works


Plaintext (64 bits)
IP
F
F
for 16 rounds
F
F
FP
Ciphertext (64 bits)
Key (64 bits)
PC1
<<<
PC2
Subkey 1
(48 bits)
Subkey 2
(48 bits)
Subkey 15
(48 bits)
Subkey 16
(48 bits)

The Feistel function (one of the 16 rounds)



An S-box

S_5		Middle 4 bits of input															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1100**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	0010	1100	0100	0001	0111	1100	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1100	0011	1001	1000	0110
	10	0100	0010	0001	1011	1100	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1100	0100	0101	0011

How to attack DES

Briefly... how to attack DES

- Differential cryptanalysis
- Linear cryptanalysis

Symmetric vs Asymmetric

Until now, the various ciphers we have discussed are known as "symmetric ciphers". It is easy to see why. However, no matter how secure the encryption is, there is always the problem of exchanging keys. Often it is either impractical or even impossible to securely exchange keys to the ciphers.

How can we get around this problem?

Public Key Systems

draw a diagram...

One-way functions : RSA and El Gamal

- Rivest-Shamir-Adleman (RSA) encryption relies on the fact that factorising large numbers of the form pq where p and q are prime numbers is very difficult compared with multiplying them together.

- El Gamal encryption relies on the difficulty of the discrete logarithm problem.

The RSA Cryptosystem

1. Choose two large prime numbers p and q such that $p \neq q$. secret
2. Set $m = pq$. public
3. Calculate $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$. secret
4. Choose an integer e such that $1 < e < \phi(n)$ such that $gcd(e, \phi(n)) = 1$. public
5. Calculate d such that $de \equiv 1 \mod \phi(n)$. secret
6. To encrypt a message, $e_K = (plaintext)^e \mod m$
7. To decrypt a message, $d_K = (ciphertext)^d \mod m$

The El Gamal Cryptosystem

1. Alice generates an efficient description of a cyclic group G of order q with generator g. public

2. Alice chooses a random x from $0, \ldots, q-1$. secret

3. Alice calculates $h = g^x$. public

4. To encrypt a message, Bob converts the plaintext (a number) into an element of G. Then he chooses a random y from $0, \ldots, q-1$, then calculates $c_1 = g^y$ and $c_2 = m \times h^y$. Bob sends the pair (c_1, c_2) to Alice.

5. To decrypt a message, Alice calculates $c_2 \times {c_1}^{-x}$

Questions?

The End

further questions, comments, email me:

largestprime@gmail.com