A Short Introduction to Encryption and Cryptology

Neil Waybright

Introduction

- An introduction to cryptography
- Focused on non-cryptographers and general audiences

Topics of Discussion

- Definitions
- Why cryptology is important
- Historic problems
- Common basic ciphers
- Problems with basic ciphers and common attacks
- Protocols and their problems
- Widely used systems

The Need for Definitions

- Common terminology is important to avoid confusion. Standards cover the usage of terms in this community
- Cryptography – the art and science of keeping messages secure.
- Cryptographers – practitioners of cryptography

Definitions

- Cryptanalysis – the art and science of reading encrypted messages not intended for them
- Cryptanalysts – practitioners of cryptanalysis
- Cryptology – the branch of mathematics that covers both cryptography and cryptanalysis

Definitions re: Ciphers

- Cipher – an algorithm used for encryption/decryption
- Encipher - the act of using a cipher to convert plaintext into ciphertext
- Decipher – the act of using a cipher to convert ciphertext into plaintext

Why Cryptography is Important

- State and military secrets
- Death or disadvantage to those that cannot do cryptography well
- Modern economic systems dependent on good cryptography
- Most computer systems authentication schemes depend on cryptographic functions

Historic Problems

- Many historic cipher systems depended on secrecy of the algorithm (Cesar and rail fence ciphers)
- No basic understanding of the underlying problems led to some poor choices based on untenable assumptions
- These problems are common today over 2000 years later

Common Basic Ciphers

- Most ciphers fall into two broad categories
  - Substitution ciphers (confusion)
  - Transposition ciphers (diffusion)
- Popular modern ciphers are variations on these two

Substitution Ciphers

- Substitution ciphers are like the cereal box decoder rings (R=A, F=B, Z=C, etc.) Each different “ring” is called an alphabet
- They can be jazzed up with multiple alphabets (first letter uses alphabet #1, second uses #2, etc.) a.k.a. polyalphabetic ciphers
- Substitution of groups of characters is referred to as polygram substitution (ALA=FQD, etc.)

Simple Substitution Example

Sample alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

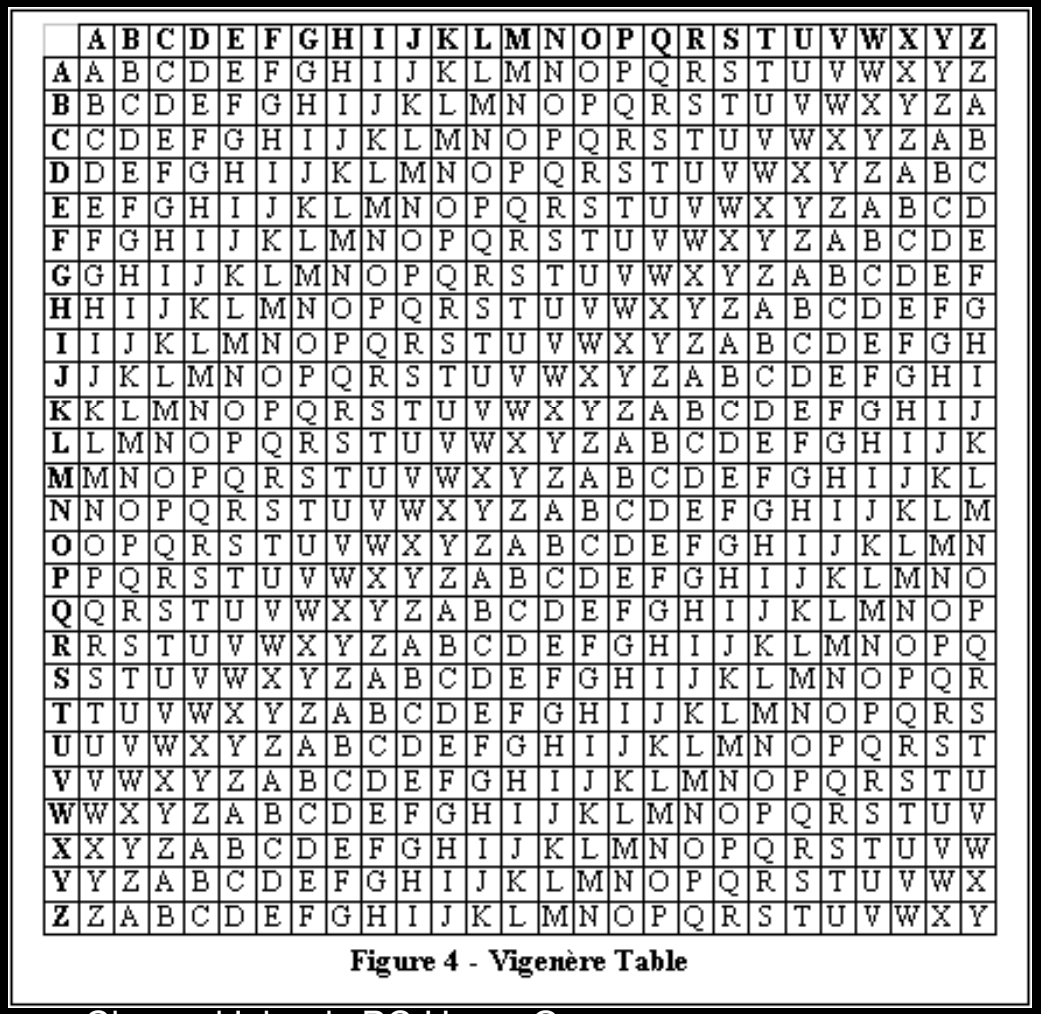
FMZKLRENAYQBXCUDGVTHSPIOHJ

ANIMAL HOUSE IS A GOOD MOVIE

becomes

FCAXFB NUSTL AT F EUUK XUPAL

Vigenère Ciphers



	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

Figure 4 - Vigenère Table

Transposition Ciphers

- Transposition ciphers use the same letters from the plaintext in the ciphertext, but change the order according to some transposition rules.
- Write in rows, read off in columns, rail fence, etc.

Simple Transposition Example

```
ANIMAL HOUSE IS
A GOOD MOVIE
```

- Becomes

```
AAN IGMOAOLD  HMOOUVSIEE  I
  S
```

XOR Based Ciphers

- In these ciphers, a key is XOR'ed or modularly combined with the plaintext to generate the ciphertext
- In trivial systems, this is a single simple word or phase.
- The length of the word or stream is termed the "period" of the cipher
- When examined using the underlying mathematics, this is simply a substitution cipher like a running-key Vigenère

Problems With Basic Ciphers

- ETAOIN SHRDLU (CMFGYP WBVKXJ QZ) is the enemy of all ciphers. The underlying letter frequency of most languages is notable and distinct.
- Unicity distance is amount of text needed to determine that the proposed plaintext is virtually certainly either readable, or gibberish. It also varies by language.

Problems with Substitution Ciphers

- Substitution ciphers are vulnerable to letter frequency based attacks. A single alphabet cipher can be broken in as little as 25 characters.
- Polyalphabetic ciphers were stronger in the days of manual attacks, but even ciphers with thousands of alphabets are easily attacked by computer programs

Problems with Transposition Ciphers

- Transposition ciphers are vulnerable to chosen and known plaintext attacks. They work best on certain “lengths” of plaintext and they require relatively large amount of memory.
- Substitution is done in S-boxes, transposition (or permutation) is done in P-boxes.

Common Attacks

- Ciphertext Only
- Known Plaintext
- Chosen Plaintext
- Adaptive Chosen Plaintext
- Chosen Ciphertext
- Chosen Key
- Rubber Hose/Purchase Key/Theft

Protocols and Their Problems

- A protocol is an exact series of steps, between two or more parties, to achieve an end goal.
- It should never be possible to achieve more, or learn more than is specified in the protocol. If it is possible, a design error is present in the protocol.
- Attacks can be active or passive, or can involve cheating.

Widely Used Systems

- DES
- AES
- BLOWFISH/TWOFISH
- RC4/ARC4
- RSA Public Key Ciphers
- Elliptical Curve Asymmetric Ciphers

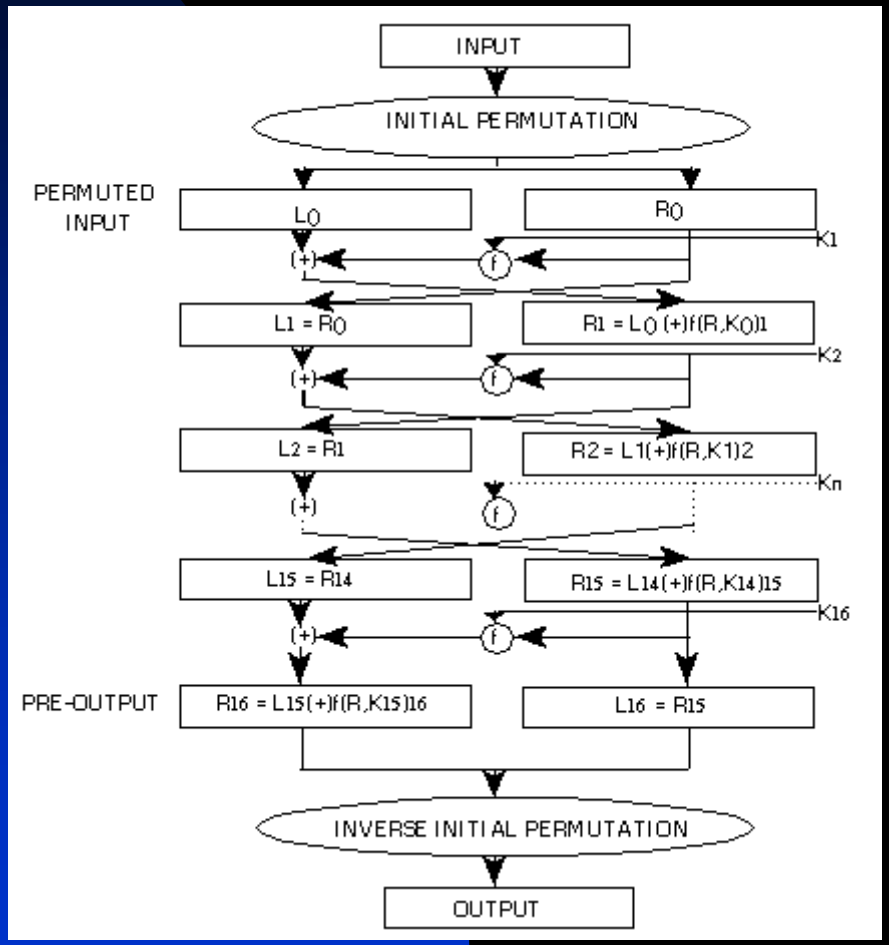
DES

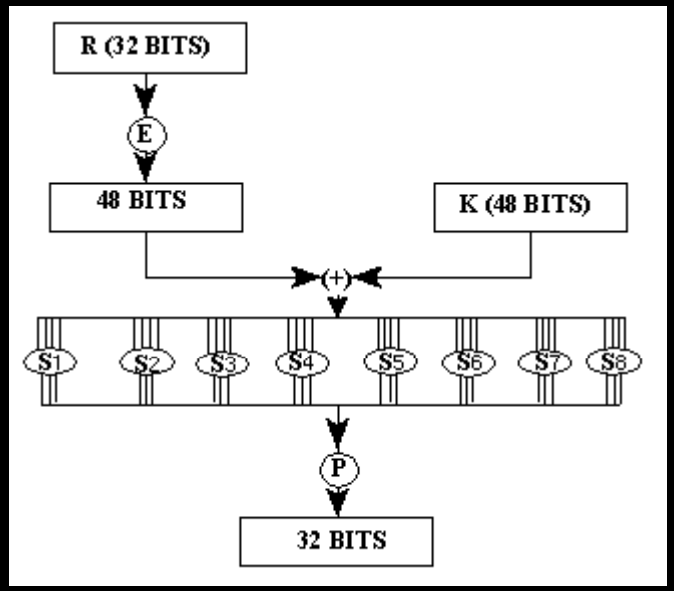
- Developed by IBM in response to a RFP by NIST for “unclassified, but sensitive data”
- Extensively researched and analyzed by one of the best crypto groups in the world outside of the NSA/KGB
- Substantial unexplained modifications were made by the NSA before the cipher was allowed in service

DES Details

- 64 bit initial key is reduced by discarding every 8th bit to yield the final 56 bit key
- There are a small number of “weak keys”, and a larger number of semi-weak keys
- Deep Crack brute-force attack successful in 22.25 hours 1998/99
- FIPS 46-3 withdrawn 5/19/2005

DES Algorithm





AES

- The Advanced Encryption Standard was sponsored by NIST as a follow-on to the highly successful DES
- Based on the Rinjdael cipher submission
- Shocked some in the community by selecting a foreign (Belgian) proposal
- 128, 192 or 256 bit key lengths

AES Details

- Uses Substitution/Permutation Network vs. Feistel Network
- No known attacks other than side-channels (timing, heat, electrical consumption)
- Recently (2003) approved for classified work up to SECRET on 128 bit keys, and TOP SECRET on 192 and 256 bit keys (HW must pass normal NSA certification)

BLOWFISH/TWOFISH

- Blowfish was designed by Bruce Schneier as a potential replacement for DES in 1993 and has no know published attacks. Initial key permutation is slow, leading it to be selected for the OBSD passwd hash algorithm

TwoFish

- Twofish was Bruce Schneier's contender for the AES proposal.
- It was slower at 128 bits, but faster at 256 bits
- Both blowfish and twofish use Feistel functions for C&D and Pseudo-Hadamard transform for additional diffusion.
- No known successful attacks

RC4

- Efficient stream cipher with notable weaknesses (no nonce, key leakage, weak IVs).
- Key component in WEP, WPA and in SSL.
- Also known as ARCFOUR in non-RSA implementations (Alleged RC-4) since the RC-4 algorithm was never officially released

RC-4 Continued

- Generally acknowledged to be ***not*** secure in general use, still safe for some restricted uses
- WPA uses TKIP and HMAC to minimize exposure to some of the algorithm's problems (and alternative algorithms)

RSA Public Key Ciphers

- Rivest, Shamir and Adleman re-invented Clifford Cock's asymmetric key ideas in 1977 while teaching at MIT.
- Security was based on the inherent difficulty of factoring large number pairs

Elliptical Curve Asymmetric Ciphers

- Based on hard number theory problem
- ECC offers considerably greater security for a given key size
- The smaller key size also makes possible much more compact implementations for a given level of security

Odds and Ends

- Steganography
- Chaffing
- Quantum cryptography
- Who knows the circumstances that the FCC allows amateurs to use encryption? (hint read 97.211(b)

Questions?