CRYPTOGRAPHY
From Black Art to Popular Science
PART 2

Fred Piper
Aims of Lecture

• To enjoy ourselves
• To look backwards and forwards
Confidentiality

How do you keep a secret?

• Don’t let anyone have access to the information
• Disguise it so that ‘unauthorised’ people cannot understand it
  – Shared secrets rely on trust
  – Trust in people, processes, technology
The ‘Secure Channel’ Concept

AIM: To send confidential information over an insecure network

• We achieve this by building a “secure channel” between two end points on the network

• Typically offering:
  – Data origin authentication
  – Data integrity
  – Confidentiality

• Cryptography is an important tool
Early Definition of a Cipher System

Message $m$ → Encryption Algorithm → Cryptogram $c$ → Interceptor → Decryption Algorithm → Message $m$

Key establishment channel (secure)
Breaking Algorithms

- Being able to determine plaintext from ciphertext without being given key
- Exhaustive key search is always (theoretically) possible

Well Designed (Symmetric) Algorithm
- ‘Easiest’ attack is exhaustive key search

Strong Algorithm
- Well designed with a large number of keys

NOTE: History is full of instances where algorithms were assumed to be well designed but ……
Warning

• If you use strong encryption and lose the decryption key then you have lost the information ‘forever’

• Danger of ‘outsourcing’ or default encryption
A Little History: Ancient Ciphers

Simple Substitution Cipher

There are $403,291,461,126,605,635,584,000,000$ keys
NOT well designed
• Frequency analysis attacks
Question: Is Simple Substitution Cipher broken?

Short answer: Yes

Challenge: If cryptogram is XAV and plaintext is 3 letter English word then what is that word?

Reality: Frequency analysis attacks only work on reasonably long messages (> 200 letters)
Breaking a Cipher

• ‘Broken’ is an emotive term
• Attacks often work only in unrealistic conditions chosen by attacker
• Always understand assumptions associated with the term
• For algorithms:
  – Ciphertext only
  – Known plaintext attack
  – Chosen plaintext attack
Early Polyalphabetic Ciphers

• Encrypt one letter using a Simple Substitution Cipher key and then change key
• Implementation was problem:
  – Difficult to make keys independent of each other
• One Time Pad
• Enigma (rotors and superencipherment)
Superencipherment and Rotation

So \( a \rightarrow D \quad b \rightarrow T \) etc

After 1 letter

\[
\begin{align*}
&I M F N W X A Z H Y L U C T V S K O R G Q P J E D B \\
&CD J R S V E L T F K G U Y O Z X W P Q N A B M I H
\end{align*}
\]

After 26 letters

\[
\begin{align*}
&B I M F N W X A Z H Y L U C T V S K O R G Q P J E D D \\
&D J R S V E L T F K G U Y O Z X W P Q N A B M I H C
\end{align*}
\]
Enigma Machine

- Polyalphabetic cipher with large period
- Day key (3 letters in code book)
- Message key (3 ‘randomly selected’ letters protected by day key)
- Problems:
  - Operators determined random selection
  - Message key sent twice
  - A message letter was never represented by itself in the cryptogram
Bletchley Park
Some Important Changes since 1945

• Advent of software
• Advent of fast computers
• Advent of new communications media
• Advent of binary codes
• Increase in general awareness
• Many applications other than provision of confidentiality
• Public key cryptography
• Seen as part of a wider discipline: Information Security
Attitudes to Cryptography

Some comparisons 1976 and 2009

1976: Cryptography was Black Art
2009: Cryptography is popular science

1976  DES: Design details secret
2009  AES: Continuous public scrutiny

1976: Strict (Enforceable) Export Control
2009: Strong algorithms freely available

Oxford 2011
Cryptographic Implementation

1976: Minimum strength to provide adequate security

2009: Maximum strength that implementation constraints allow

During this period cryptography has become recognised as part of a much wider topic: Information Security
Popular Does Not Mean Easy

• Golf is a popular sport
• Anyone can swing a golf club
• Occasionally a complete novice will hit a good tee shot
• Being a professional is hard work
  – Training
  – Practice
Royal Holloway: Our Most Famous Ex-Student?
Two of the Most Significant Cryptography Publications since 1975

New Directions in Cryptography:
Diffie, W. and Hellman, M.E.

*Trans IEEE Inform. Theory. IT-22*
644-654, November 1976

Federal Information Processing Standards Publication 46
Announcing the DATA ENCRYPTION STANDARD
January 1977
Kerchoff’s Principle

• The security of a cryptographic system should not depend on keeping the encryption algorithm secret

It does not say

• The encryption algorithm should be made public

However

• Anyone assessing the security of a cryptographic system needs to have confidence that the algorithm is strong
Some Principles

- Security by obscurity is unsafe
- Obscurity can help security
A Never Ending Debate

• What gives us confidence in an algorithm?
  – Standards?
  – Ask the opinions of experts?

• Early debate
  – Publicly known or proprietary algorithms?
  – Less of an issue now than in the 1980s

WARNING

The fact that an algorithm is published and unbroken says nothing about its strength
Recognising Well Designed Algorithms

Some issues

• No proof of security for symmetric algorithms
• What is role of referee if encryption algorithm is submitted for publication?
• Why do academics try to break algorithms? Is it worth it for them?
• Early publications attacked DES, but some other published algorithms were not publicly attacked
• What would have been the consequences if someone had broken DES in the 1980s?
It is NOT just about Algorithms

Early 1980s:
• Thorn EMI conference
  “Security is People”

Early 1990s:
• Ross Anderson’s paper
  “Why crypto systems fail”
Use of Cryptographic Algorithms

- An algorithm has many uses
- Adaptation by modes of operation
- Protocols to apply the algorithm
- Design of secure protocols
- Key Management supports it
Misuse of Cryptography

Good student

Bad student

Grades can be changed

Oxford 2011
Cryptographic System

- The use of strong algorithms prevents attackers from calculating or guessing keys
- Keys need to be stored and/or distributed throughout the system
- Keys need protection
Protecting Keys (Storage or Distribution)

- Physical security
  - Tamper Resistant Security Module (TRSM)
  - Tokens (Smart Cards)
  - Armed guards

- Components
  - Secret Sharing Scheme

- Key hierarchies
  - Keys encrypted using other keys
  - Lower level keys derived from higher level ones
Side Channel Attacks

To find a cryptographic key

• **Exhaustive key search attacks** try to find the secret key by random trial and error

• **Side channel attacks** try to use additional information drawn from the physical implementation of the cryptographic algorithm at hand so as to be substantially better than trial and error
Dec 11, 1995: Paul Kocher announces timing attack on the sci. crypt news group:

“I’ve just released details of an attack many of you will find interesting since quite a few existing cryptography products and systems are potentially at risk. The general idea of the attack is that secret keys can be found by measuring the amount of time used to process messages. The paper describes attacks against RSA, fixed exponent Diffie-Hellman, and DSS, and the techniques can work with many other systems as well”.
Control of Encryption

The widespread use of encryption for confidentiality has always been a cause of concern for Governments.

Over simplification of objectives

- To provide strong encryption for use for ‘good’ purposes
- To be able to break encryption used for ‘bad’ purposes
Saints or Sinners?

Who are the ‘good’ guys?
Governments’/Law Enforcement’s Dilemmas

• Do not want to intrude into people’s private lives
• Do not want to hinder e-commerce
• Want to have their own secure communications
• Occasionally use interception to obtain information
• Occasionally need to read confiscated, encrypted information
Control of Encryption

Export Control
- Easier in 1970s and 1980s
- The application process has changed
- Black Box Deception no longer possible (trapdoors)

Key Escrow
- Offers secrecy from everyone except Government (in special circumstances)

Regulation

NOTE: If someone wants your key they might
- Break the algorithm
- ‘Find’ the key in the system
- Be given it
Black Box Deception

- Randomness
- Prime generation
- Reduce effective key search
Loss of Control of Encryption

• Academic papers
  – Attacks on DES
  – New algorithms
• Text books
• Need for international systems
Newton Minow, Speech to the Association of American Law Schools, 1985

• After 35 years, I have finished a comprehensive study of European comparative law

• In Germany, under the law, everything is prohibited, except that which is permitted

• In France, under the law, everything is permitted, except that which is prohibited

• In the Soviet Union, under the law, everything is prohibited, including that which is permitted

• And in Italy, under the law, everything is permitted, especially that which is prohibited
The Political Breakthrough

- GSM
- ETSI produced (shared) encryption algorithm for Europe
- Designed to be as secure as the existing ‘land line’ network
Authentication

• It is important to authenticate people and devices
• Man-in-the-Middle Attacks
• How to beat a Grand Master at chess
User Recognition Methods

1. Something known by user (eg PIN, password)
2. Something owned by user (eg smartcard)
3. Biometric property of user

**NOTE:** At least 2 and often all 3 of these methods are combined
User Authentication Using Symmetric Cryptography

Can only take place between two parties who are prepared to co-operate with each other

Typical scheme:

A and B share a secret key $K$ which (they believe) is known only to them

If A receives a message encrypted with key $K$ then A believes that the message originated from B

Note: A and B need to protect against replays etc
New Directions in Cryptography: 1975

• **Conventional or Symmetric**
  – Decryption key easily obtained from encryption key

• **Public or Asymmetric**
  – Computationally infeasible to determine decryption key from encryption key

**NOTE:** CESG initially referred to this as non-secret encryption
Mortice Lock
If you can lock it, then you can unlock it

Bevelled Sprung Lock
Anyone can lock it, only keyholder can unlock it
• User is only person who can use private key
• Anyone can use public key to check that a private key was used
Attacks on Public Key System

To impersonate you I may either:
• Obtain your private key
• Get my public key accepted as yours

Defence need Public Key Infrastructure (PKI)
• Significant overhead
• Trusted third party
A Fact of Life!

• In theory there is no difference between theory and practice. In practice there is.
RSA: The Theory

- The published modulus is the product of 2 secret primes
- Knowledge of the secret primes makes it easy to find the private key
- In general, determining the private key appears to require knowledge of the primes
- Factorisation is difficult
- So, for large moduli, RSA is secure
RSA: In Practice

- Early implementations used prime generation with only a million primes
- Exhaustive prime searches were possible
- The theory was irrelevant!
Is Cryptography built on a ‘sound’ basis?

“Many cryptographic systems rely on the inability of mathematicians to do mathematics”.

(Donald Davies: LMS Lecture)

Tongue in cheek?

Existence proofs do not provide solutions
Algorithms should be implementable
Accuracy of Information

• Information on a database is useless unless it is accurate
• Prevention of alteration
  – Deny access
• Detection of alteration
  – Cryptographic check sum
    • Digital signatures
    • MACs
Dispute Resolution

• Symmetric systems
  – No (cryptographic) dispute resolution between 2 key holders
  – Protection against 3rd parties only, not each other

• Digital signatures
  – Need asymmetric system
  – PKI overhead?
Hand-Written Signatures

- Intrinsic to signer
- Same on all documents
- Physically attached to message
- Beware plastic cards.

• Digital Signatures
  - Use of secret parameter
  - Message dependent.
What is a Binary String?

A bit string of length $s$
1. A string of bits
2. An integer for 0 to $2^s - 1$
3. A sequence of integers
4. Coordinates to a look-up table
5. Vector in $V(s,2)$
6. Binary polynomial (degree at most $s - 1$)
7. Indicator set for integers 0 to $s - 1$
8. Your choice?
Classification of Techniques

Bit / Block operation
Message dependence/independence
Positional dependence/independence
Error Propagation

If the decryption process has the property that accepting an input with 1-bit in error produces an output with more than 1 unreliable bit, then we say there is ERROR PROPAGATION

• Block encryption leads to error propagation
Vernam Cipher

Random sequence \( k_1, k_2, \ldots, k_n \)

Message \( m_1, m_2, \ldots, m_n \)

Ciphertext \( k_1 \oplus m_1, k_2 \oplus m_2, \ldots, k_n \oplus m_n \)

The message and key are bit strings
One-Time Pad

- At least as many keys as messages
- Each key used only once
- Provably unbreakable
- Key management problems
- Requires second communications channel for the key
- Not suitable for most applications
Stream Cipher

Plaintext data → Key

Key → Sequence Generator

Sequence Generator → Keystream sequence

Keystream sequence → Modulo 2 addition

Modulo 2 addition → Ciphertext
Stream Ciphers

Applications

• Widely used for military and paramilitary applications for both data and digitised speech
• The main reason for their wide use is that military communications are often over poor channels and error propagation is unacceptable
Symmetric Block Cipher System

Key dependent permutation on s-bit blocks

s-bit plaintext block

Key

s-bit ciphertext block
ECB Mode for a Block Cipher

To encrypt a message $m$ using a block cipher with block size $s$

(a) Divide the message into ‘blocks’ of $s$-bits
(b) Use padding (with agreed convention) if needed to ensure that the ‘last’ block has $s$ bits
(c) Encrypt each block individually

NOTE: Identical message blocks give identical cryptogram blocks
Fast DES Key Search

DES has 56-bit key

DES Breaker used with Internet search
Key found in less than a day
Consequences

The use of single length DES cannot be justified for protecting ‘valuable’ information with a cover time of more than a few minutes.
There are several different proposals for 3DES

Typical deployments use 2-key or 3-key EDE
DES Conclusions

• We believe that DES is a well-designed cipher
• Best attack is exhaustive search – 30 years after design
• Exhaustive search is practical
• Enter AES (2002)
64-bit Key Search

- RC5 secret key challenges
- Key found 26.9.02
- Took about 4 years
- Task undertaken by distributed network
- Used 331,252 volunteers
Future Developments?

• Steganography
  – You hide information rather than distort it
  – Harder to detect?

• Quantum
  – Quantum key establishment
  – Quantum cryptography
  – Quantum computing

• Provable security
  – Academic ‘dream’ or reality?

• Default encryption
  – Who looks after keys? (liability issues)
ARTICLE 8: RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

1. Everyone has the right to respect for his private and family life, his home and his correspondence
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others.
Human Rights Statements

Some problems

- What does the caveat mean?
- Who decides when the exceptions are justified?
- Finding a balance between rights and responsibilities