Fred Piper

Information Security Group

Royal Holloway
University of London

Cryptography

From Black Art
to
Popular Science

Fred Piper

Codes & Ciphers Ltd
12 Duncan Road, Richmond
Surrey, TW9 2JD
Fred.piper@codesandciphers.net

Royal Holloway, University of London
Egham Hill, Egham
Surrey TW20 0EX
f.piper@rhul.ac.uk
www.isg.rhul.ac.uk

Aims of Lecture

- To enjoy ourselves
- To look at some implementation issues for cryptographic systems
- To see how cryptography has changed in the last 40 years

Industry’s Problems with Implementing Cryptography

- No real problems with algorithms – it’s the wraparounds
- Serious concerns about some recent events – DigiNotar, RSA
- Not sure how they should be regarding possibility of quantum computers
- Cryptography needs standards (change slowly), but we need flexibility
- Need for early warning about necessary changes (e.g. key lengths)
- Concerns about timeliness of hardware (cryptographers recommend changes faster than hardware can be replaced)

A Little History

- **Pre-1975: Hush hush!**
  – Practised mainly by Governments and military
- **Early 1980s: Courses start**
  – Customers start to know what they require
- **Early 1990s: Qualifications start**
  – The role of security manager is no longer a punishment
- **Early 2000s: Popular science**
  – Everyone knows about it
- **Today: Fundamental to e-commerce, e-Government etc**

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 short
- Being a professional is hard work
  - Training
  - practice

Royal Holloway: Our Most Famous Ex-Student?

Why is the Profile of Encryption Growing?

- Increase in volume of communications over insecure channels
- Increased requirement for remote access to information
- Regulatory requirements for ‘adequate’ protection of data
- Need for electronic ‘equivalent’ to handwritten signatures and other forms of identification
- It can be fun!

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

What is Information Security?

Information Security includes the following three aspects:

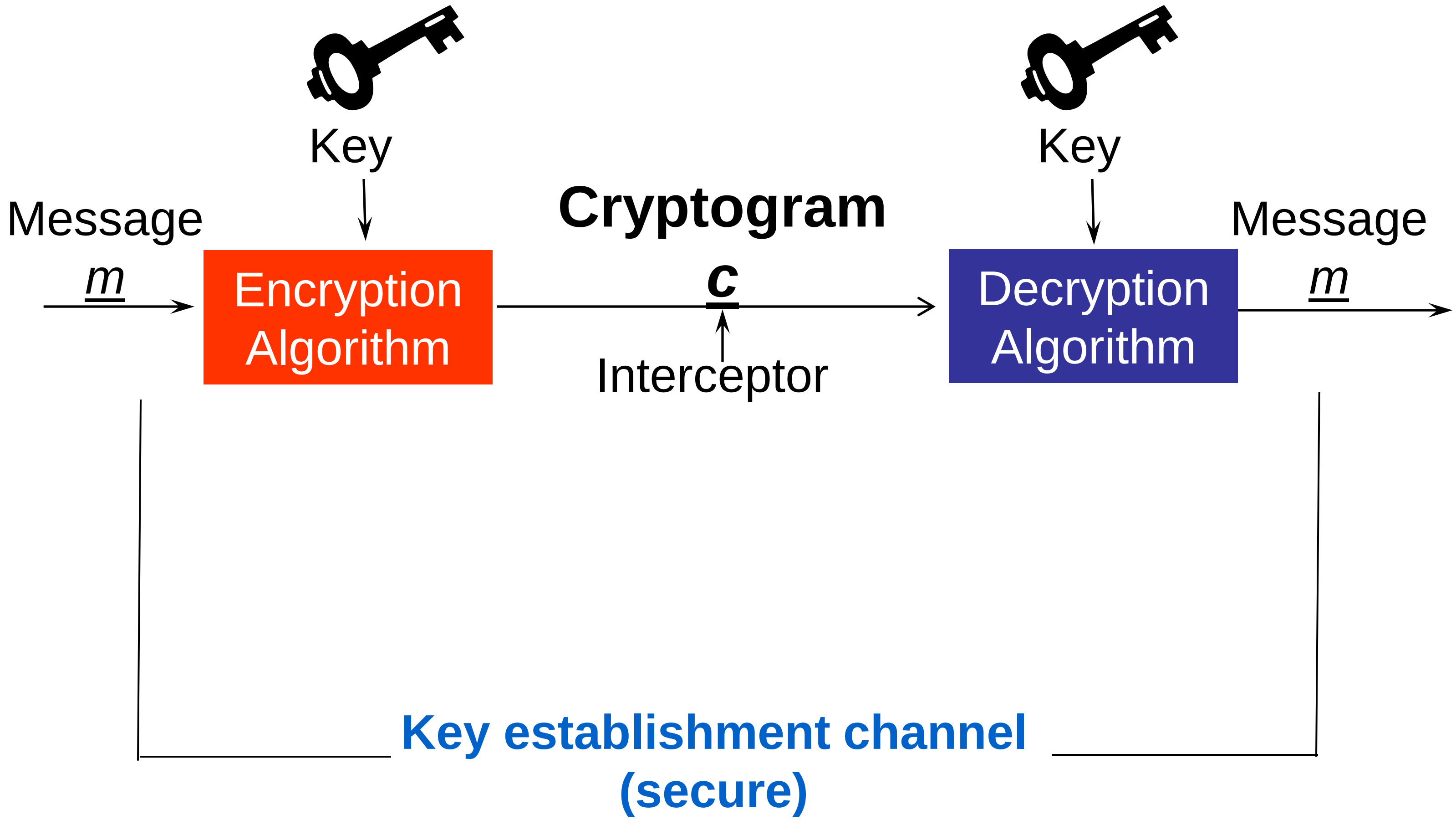
- **Confidentiality**
  - Protecting information from unauthorised disclosure, perhaps to a competitor or to the press
- **Integrity**
  - Protecting information from unauthorised modification, and ensuring that information, such as a customer list, can be relied upon and is accurate and complete
- **Availability**
  - Ensuring information is available when you need it

NOTE: Impersonating an authorised user is often a more effective form of attack than ‘breaking’ the technology

Authentication

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

Early Definition of a Cipher System



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
- **If you use cryptography to protect your information then there will be a key to which you must deny access**

Warnings

- If that key is lost and the algorithm is strong then your data is lost ‘forever’
- If someone else gains access to that key then they almost certainly have access to your information

Breaking an Algorithm

- 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 ……

Breaking a Security System

- ‘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

The ‘Secure Channel’ Concept

AIM: To send information securely 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

Disclaimer: Cryptography ≠ Security

- Crypto is only a tiny piece of the security puzzle
  - but an important one
- Most systems break elsewhere
  - incorrect requirements or specifications
  - implementation errors
  - application level
  - social engineering

Security Breaches

Many Reasons:

- Badly designed systems
- Inappropriate policies
- Human error
- Clever, innovative (technical) attacks
- Misplaced trust (e.g. In employees or trusted third party)

Attacking Cryptographic Systems

- Passive interceptor attempts to break algorithm
- Active interceptor has more options
- Interception not necessarily the 'best' form of attack
  - Attack protocols
  - Attack key management
  - Attack the hardware
  - Impersonate genuine users
  - Espionage

Is PK 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

Are Today’s Algorithms ‘Future Proof’?

- **Symmetric algorithms**
  - if well designed then key searches are ‘best’ attacks
  - Main concern is advances in technology
  - Moore’s Law
- **Asymmetric algorithm**
  - Always concerned about mathematical advances
  - Quantum computing
- **Hash functions**
  - Confidence shaken

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

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

So:

- Financial institutions should use public algorithms where appropriate

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

Attacks on RSA

The theory assumes that the attacker will need to factor *n* using a mathematical factorisation algorithm

In practice this may not be so

EARLY ATTACKS

Attack prime generator rather than try to factor *n* mathematically

(1) Exhaustive prime search

(2) Exploit bias in generation process

Progress?

- So have we learnt from these early mistakes?

In theory:	YES
In practice:	NO

‘Shared’ Primes

- Factoring RSA moduli is very difficult
- Finding g.c.d. of two RSA moduli is easy
- Factoring two RSA moduli which share a prime factor is easy
- Recent research showed that, for a sample 6.6 million RSA keys, over 4% either have a common modulus or gave moduli sharing a common prime factor
- Suspect prime generators?

“Ron was wrong, Whit is right”

“When exploited it could affect the expectation that the public key infrastructure is intended to achieve”

(Arjen K Lenstra, James P Hughes et al)

It is NOT just about Algorithms

Early 1980s:

- Thorn EMI conference

  "Security is People"

Early 1990s:

- Ross Anderson's paper

  "Why crypto systems fail"

Cryptographic Systems

- 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)
- Components
  - Secret Sharing Scheme
- Key hierarchies
  - Keys encrypted using other keys
  - Lower level keys derived from higher level ones

Side Channel Attacks (1)

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**

Side Channel Attacks (2)

- Changed the way cryptographers think about security
  - Properties of digital circuits are far more important for security than was previously believed
    - Many previous design approaches recognised as inadequate

Some Recent ‘Changes’

- More attacks concentrate on the implementation of the algorithm and the accompanying protocols
- Some exploit error messages
- Academic research is becoming less ‘blue skies’ and focussing on real systems/problems
- Theory and practice are getting closer to each other

Error Messages

ATM transaction

- Incorrect PIN
- Insufficient funds in account
- Exceeded daily limit

Public Key Infrastructures

- Certification Authorities
- Sign certificates to bind user's ID to their public key
- Hierarchy of CAs
- Root CA at top of hierarchy

NOTE: If root CA's private key is compromised then the entire PKI is affected

DigiNotar

- Netherlands based CA
- Host many other CAs
  - SSL certificates
  - Qualified certificates
  - Government accredited
- Hackers gained unauthorised access to their CA servers
- Issued series of rogue certificates

SERIOUS BREACH: DigiNotar root certificate was trusted by most widely used web browsers and email clients

Hacker set up spoof websites (e.g. Googlemail)

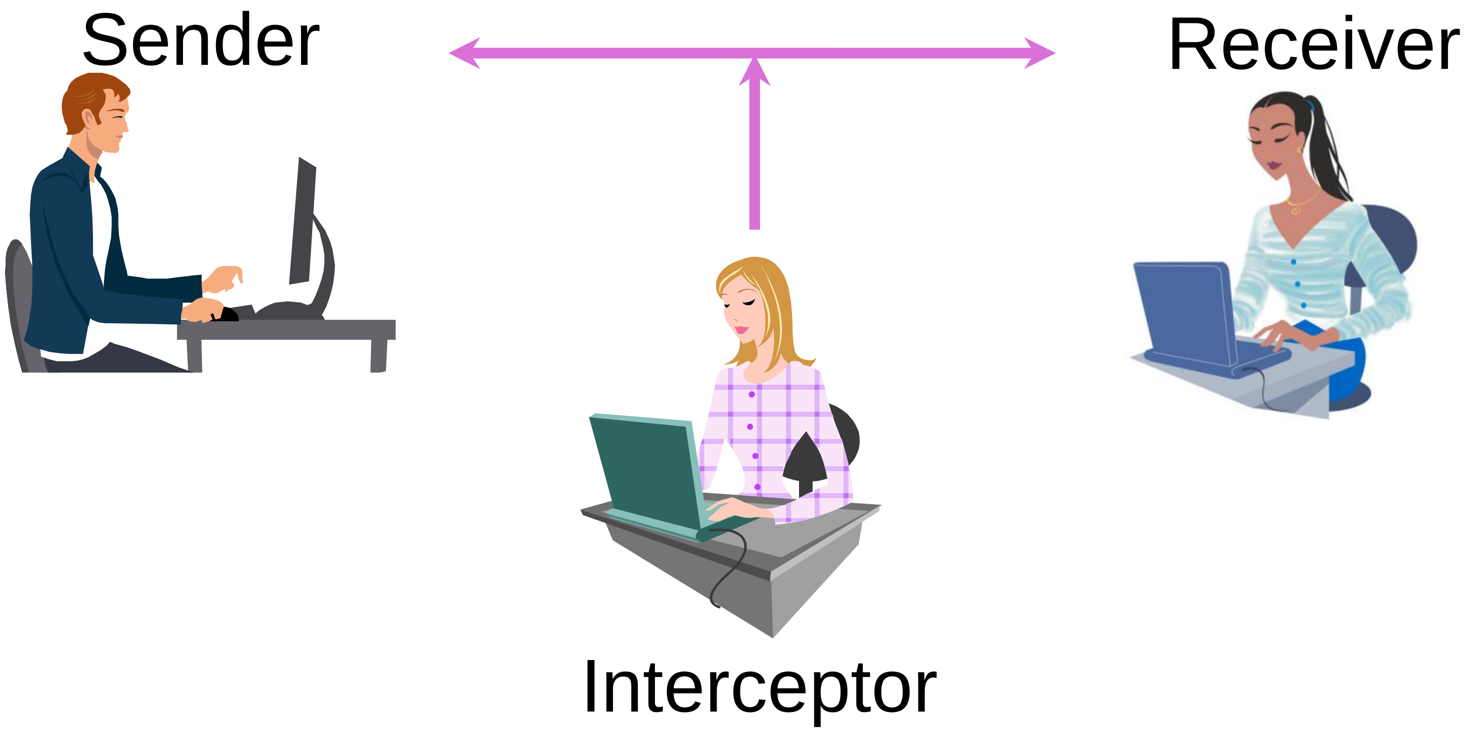
Problem

- Who, or what, can we trust?

Some Things Never Change

- The widespread use of encryption for confidentiality has always been a cause of concern for Governments
- Simplified version of Government’s position
  - They are happy to support the use of strong encryption for ‘good’ purposes
  - Unhappy about the use of strong encryption for ‘bad’ purposes

Saints or Sinners ?



Who are the 'good' guys ?

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

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