Assignment 1 is due tomorrow.

Assignment 2 is due on Thursday 11 Nov.
This session

- Hamming revision...

- Protocols
  - Kerberos
  - Voting
  - Tossing a coin
  - Contracts

- Ethics

Hamming revision

The *hamming* distance is a measure of how FAR apart two bit strings are.

A: 0 1 0 1 1 1 0 0 0 1 1 1
B: 0 1 1 1 1 1 1 0 0 1 0 1
A XOR B: 0 0 1 0 0 0 1 0 0 0 1 0

(In this case: 3)
Single correct \(n(=4)\) bit code

Incorrect codes. (\(n=4\) of them)
Each with a hamming distance of 1 away from the correct code.

✔ So ... with an \(n\)-bit code, there will be 1 correct code, and \(n\) codes 1 bit away.

✔ For 1-bit correction, we want these all to be unique, so to represent \(2^m\) symbols we will have \((n + 1)2^m\) codes.

✔ The total number of codes is \(2^n\), so \((n + 1)2^m \leq 2^n\).
Hamming Q1

1. Calculate the minimum extra bits needed for encoding a 32 bit value, with two-bit error detection. Show your own worked version of the Hamming calculation in the notes.

**Answer:** This requires us to use the equation in the book. We want a hamming distance of 3, so

\[
(n + 1)2^m \leq 2^n \\
32 + 1 \leq 2^r - r \\
R = 6
\]

Hamming Q2

2. Calculate the minimum extra bits needed for encoding a 32 bit value, with two-bit error correction. Show your own worked version of the Hamming calculation in the notes. Note that in this case we want to do error recovery, not error detection.
Hamming Q2

The number of illegal encodings is \( \frac{n^2 + n}{2} \), and so our inequality becomes:

\[
\left( \frac{n^2 + n}{2} + 1 \right) 2^m \leq 2^n
\]

\[
\left( \frac{(m + r)^2 + (m + r)}{2} + 1 \right) 2^m \leq 2^n
\]

\[
\frac{(m + r)^2 + (m + r)}{2} + 1 \leq 2^{n-m}
\]

\[
\frac{m^2 + 2rm + r^2 + m + r + 2}{2} \leq 2^r
\]

Then, given \( m = 32 \), we can calculate

\[
\frac{1024 + 64r + r^2 + 32 + r + 2}{2} \leq 2^r
\]

\[
1024 + 64r + r^2 + 32 + r + 2 \leq 2^{r+1}
\]

\[
1058 \leq 2^{r+1} - 65r - r^2
\]

\[
R = 10
\]

So we have that the minimum number of extra bits for a 32 bit encoding to do 2-bit error recovery is 10.
This session

- Hamming revision...

- Protocols
  - Kerberos
  - Voting
  - Tossing a coin
  - Contracts

- Ethics
A voting protocol is one in which

- independent systems vote in a kind of election, and
- afterwards we can check that the vote was correct.
- Each voter is only allowed a single vote, and
- the system should be corruption-proof.

Example with Alice, Bob and Charles (!), who vote and then encrypt and sign a series of messages using public-key encryption. For example, if Alice votes $v_A$, then she will broadcast to all other voters the message

$$R_A(R_B(R_C(E_A(E_B(E_C(v_A))))))$$

where $R_A$ is a random encoding function which adds a random string to a message before encrypting it with $A$’s public key, and $E_A$ is public key encryption with $A$’s public key.
Each voter then **signs** the message and **decrypts** one level of the encryption.

At the end of the protocol, each voter has a complete **signed audit trail** and is ensured of the validity of the vote.

---

**This session**

- Hamming revision...
- Protocols
  - Kerberos
  - Voting
  - Tossing a coin
  - Contracts
- Ethics
Alice and Bob want to toss a coin

Alice calculates two primes $p, q$ and calculates $N = pq$, sends $N$ to Bob. $N = 35 = 5 \times 7$

If Bob can factorize the number, then Bob wins a coin toss.

Bob selects random $x$, and sends $x^2 \mod N = y$ to Alice. $y = 31^2 \mod 35 = 16$

Alice calculates the four square roots of 16:

- $4^2 \mod 35 = 16$
- $31^2 \mod 35 = 16$
- $24^2 \mod 35 = 16$
- $11^2 \mod 35 = 16$

This is easy for Alice, as she knows the prime factors of $N$. She then sends one of these back to Bob.
Tossing a coin

✔ If Bob receives $x$ or $-x$, then he learns nothing, but

✔ if Bob receives either of the other values, he can add this to $x$, and then find the GCD of the result with $N$:

\[
\text{GCD}(24 + 31, 35) = \text{GCD}(55, 35) = 5
\]

✔ Alice is unable to tell she has divulged the factor

This session

• Hamming revision...

• Protocols
  – Kerberos
  – Voting
  – Tossing a coin
  – Contracts

• Ethics
Oblivious transfer

✔ In an oblivious transfer, randomness is used to convince participants of the fairness of some transaction

✔ In a coin-tossing example, Alice knows the prime factors of a large number, and if Bob can factorize the number, then Bob wins a coin toss.

✔ A protocol allows Alice to either divulge one of the prime factors to Bob, or not, with equal probability.

✔ Alice is unable to tell if she has divulged the factor, and so the coin toss is fair.

Contract signing

✔ Signing contracts can be difficult.

✔ If one party signs the contract, the other may not. We have one party bound by the contract, and the other not.

✔ In addition, both may sign, and then one may say “I didn’t sign any contract!” afterwards.
Contract signing

Oblivious transfer used for contract-signing where

- Up to a certain point neither party is bound
- After that point both parties are bound
- Either party can prove that the other party signed

Alice and Bob exchange signed messages, agreeing to be bound by a contract with ever-increasing probability.

- ✔ In the event of early termination of the contract, either party can take the messages they have to an adjudicator, who chooses a random probability value (42% say) before looking at the messages.
- ✔ If both messages are over 42% then both parties are bound.
- ✔ If less then both parties are free.
This session

- Hamming revision...
- Protocols
  - Kerberos
  - Voting
  - Tossing a coin
  - Contracts
- Ethics

CS3235 - Hugh Anderson's notes. Page number: 464

Stranger danger...

One of my sons was taught stranger-danger at his school. We were asked to quiz him afterwards, so we asked him if he should accept a lift in a car with a stranger. He immediately replied “No way!”. We then asked: “What if he offered you sweets?”, but he still replied “No way!”. Finally we asked: “Why not?”, to which he replied “Because you might not get any!”

CS3235 - Hugh Anderson's notes. Page number: 465
Moral development stages:

**Stage 1:** *Obedience and punishment*

... 

**Stage 6:** *Individual principles of conscience* - an orientation not only toward existing social rules, but also toward the conscience as a directing agent, mutual trust and respect, and principles of moral choice involving logical universalities and consistency. If one acts otherwise, self-condemnation and guilt result.

✔ It is my expectation, and requirement, that you are able to maturely evaluate rights and wrongs.

✔ In these sections of the course, I will be outlining systems which demonstrate poor cryptographic techniques, and as a result, can be defeated.

✔ A more cynical view might be that we are *hacking*  

...this is not my intent...
No new ethical dilemmas... Perhaps the only significant difference is that the computer crimes are so easy.

**Software duplication:** = *theft.*

**Using information:** = *insider trading.*

**E-mail abuse:** = *abuse.*

---

**Network administrator’s dilemma**

✔ Network administrators often come to learn things about their ’clients’

✔ Without asking the client, they should not make use of that information.

✔ The network administrator’s dilemma: How to control bad-guys without trampling over rights.
Professional codes of ethics

✔ Most professional bodies\textsuperscript{19} have formal written codes of ethics

✔ The computer industry has yet to develop a standard code of conduct

✔ If computer crime continues to rise, codes may be imposed on it.

\textsuperscript{19}For example: Medical boards.

ACS code of ethics

1. I will serve the interests of my clients and employers, my employees and students, and the community generally, as matters of no less priority than the interests of myself or my colleagues.

... Within a general framework of ethical and moral responsibility, codes such as this one can help clarify grey areas of concern.
Insecurity - threats are real

For example:

- Pentagon machines were repeatedly corrupted by unknown intruders during the Gulf war. The intruders appeared to be doing it as part of a contest.

- German hackers demonstrated on TV a method of transferring money into their own accounts using ActiveX controls downloaded to an unsuspecting person’s machine.

- Estimates of computer theft in the US range from 1 to 30 $billion/year - most of which goes unreported.

Taxonomy of insecurity?

Each new attack adds new levels to the structure:

- physical insecurity, and

- password insecurity

Some of the security of modern systems is provided through cryptographic techniques (particularly password storage), the subject today.
Non-cryptographic cracking

**Misconfiguration:** If excessive permissions exist on certain directories and files, these can lead to gaining higher levels of access. For example, on a UNIX system, if /dev/kmem is writable it is possible to rewrite your UID to match root’s.

**Poor SUID:** Sometimes there are scripts (shell or Perl) that perform certain tasks and run as root. If the scripts are writable by you, you can edit it and run it.

---

Buffer overflow: Buffer overflows are typically used to spawn root shells from a (server) process running as root.

**Race conditions:** A race condition is when a program creates a short opportunity for attack by opening a small window of vulnerability. For example, a program that alters a sensitive file might use a temporary backup copy of the file during its alteration.
Non-cryptographic cracking

**Poor temporary files:** Many programs create temporary files while they run. If a program runs as root and is not careful about where it puts its temporary files and what permissions these files have, it might be possible to use links to create root-owned files.

Attacks using these methods can be launched *locally* on the target machine, or often *remotely*, by exploiting *services* with loopholes.

---

Protection

Can you protect yourself against attacks?

- **Hack/crack yourself:**
- **Be vigilant:**
- **Reduce reliance:**
- **Use more secure systems:**
- **Update systems:**

Finally: “*Its not the end of the world!*”
The CERT Coordination Center is the organization that grew from the computer emergency response team formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 in response to the needs identified during the Internet worm incident. The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community’s awareness of computer security issues, and to conduct research targeted at improving the security of existing systems.

If you are ever involved in a computer security incident it is useful to get in touch with CERT.

They provide incident reports and advisories, and can liaise with other system administration people if the attack on your system comes from outside your organization.
Here is an excerpt from an incident report:

**Similar Attacks Using Various RPC Services**

Thursday, July 22, 1999

**Overview**

We have recently received an increasing number of reports that intruders are using similar methods to compromise systems. We have seen intruders exploit three different RPC service vulnerabilities; however, similar artifacts have been found on compromised systems.

...

---

**SIGINT**

✔ *Signals Intelligence* (SIGINT) broke the Japanese military code and learned of plans to invade Midway Island.

✔ In 1943 they began the VENONA project to examine encrypted Soviet diplomatic communications.

✔ The messages were double-encrypted and were extremely difficult to crack.

✔ Almost all of the US KGB messages in 1944 and 1945 were broken between 1947 and 1952.
The National Security Agency is the USA's cryptologic organization.

It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information.

NSA employs the country's premier codemakers and codebreakers.

It is said to be the largest employer of mathematicians in the United States and perhaps the world.
Rainbow documents

✔ The NSA created various documents describing the criteria for evaluating the security behaviour of machines.

✔ These criteria were published in a series of documents with brightly coloured covers, and hence became known as the Rainbow series. (red book, yellow book...)

C2 security


- To provide a standard to manufacturers (for security features related to confidentiality)...

- To provide DoD components with a metric with which to evaluate the degree of trust...

- To provide a basis for specifying security requirements in acquisition specifications.
C2 security example

✔ The TCB\textsuperscript{20} shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate.

✔ Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity.

\textsuperscript{20}Trusted Computing Base.

---

Microsoft and C2

Windows NT Workstation vs 3.5 with U.S. Service Pack 3 was the first Microsoft product that has completed C2 testing, and is only certified if using the same hardware, and installed software, and does not include any network connection. The NT utility \texttt{c2config.exe} sets up an NT system to pass the C2 tests.

\textit{The 1998 attacks on the Pentagon involved theft and modification of data, as well as denial-of-service. The attacked machines were C2-secure Windows NT machines.}
UNIX and C2

Many UNIX systems have also got C2 certification, and come configured this way from the manufacturer.

There are numerous examples of hacked UNIX systems found on the Internet. In 1996, a site I managed in New Zealand was the target of a malicious attack by intruders from Australia and Belgium.

Given all this, C2 certification is probably not a good guide as to the security of your system.