**This document is best used with search

COMP6[48]41 Course Textbook

Table of Contents

Table of Contents **2**

MODULE #01 **9**

Security engineering - what is security engineering? 9

The asymmetry between attackers and defenders. 9

Digression: Algorithmic verification 10

History of hacking 10

Security Flaw Types 10

Crypto Literacy 11

MODULE #02 **12**

Recon 12

Active vs Passive 12

Dumpster diving 12

Shredding paper 12

Google disposal 12

The problem of security 13

How do we build a secure system? 14

Engineering Approach 15

Type I and Type II Errors 15

Protocols - CIA 16

Cryptographic Primitives 17

Properties of Cryptographic Primitives 17

Jargon 17

Bits of Security 18

Ciphers 19

Old Codes 20

Substitution Cipher 20

Transposition Cipher 21

Solving a Cipher 21

Cipher Handbook 22

MODULE #03 **26**

Risk 26

Approaches to dealing with risks 26

Keys / 26

Merkle's Puzzles 27

One Way Function 28

Math Review 29

Diffie Hellman Key Exchange 29

How it works 29

RSA 30
How it Works 31
Another Explanation 31
Worked examples 32
Euclid's Algorithm 34
MODULE #04 35
Human Weakness 35
Examples of human weakness 37
Physical Security 38
Hashing 38
Hashing vs Encryption: 39
Cryptographic Hash Properties 39
Hashing Attacks 39
Preimage attack 39
Second Preimage Attack 39
Birthday Attack (Attacking the Hash's Collision resistance) 40
Hashing Attack Examples 40
Hashing Attacks Pictorially 40
Hashing Algorithms 41
MAC - Message Authentication Code 41
NONCE 41
Length Extension Attacks 42
MODULE #05 43
Vulnerabilities and exploits 43
Bug Types 43
Exploits 43
Common bugs 44
Common Vulnerabilities and Exposures (CVE) 44
Assets 44
Strategies for identifying assets 45
Examples of Assets 45
Bits of Security 46
Entropy 46
Example 46
Another Example 46
Hash Properties 47
Sessions 48
Session Timeouts also known as "Reaper Timeouts" 48
Session Hijacking 48
Deep Packet Inspection 49
Digital signatures 49

Keys (Revisit) 50
Birthday Attack Example (revisit) 50
Lessons from the birthday paradox 51
How to protect yourself against the birthday attack 51
Birthday Paradox 52
Pre-Image Attack Recap 52
Looking at military weapons 53
MODULE #06 **54**
One-Time Pads 54
The Process 54
Properties 54
XOR 54
More on XOR 55
XOR Encryption 55
Confusion and Diffusion 56
Symmetric and Asymmetric Encryption 56
Symmetric Cryptography 56
Asymmetric Cryptography 56
Symmetric Encryption 57
A symmetric encryption scheme has 5 ingredients: 57
Requirements for secure use of symmetric encryption 57
Symmetric Encryption Attacking Approaches 58
Symmetric Block Encryption Algorithm 58
Symmetric keys 59
DES 59
Concerns on Strength of DES 61
AES (Rijndael) 192, 61
Analysis of FingerPrints 67
MODULE #07 **69**
ACSC survey 69
Knowledge is power 69
Side channel attacks 70
Examples 70
General Classes of Attack 71
"Top men" 72
Examples 72
Security lessons 72
The process for a security assessment: 72
Building up a Threat Model 72
Threat Trees 73
Dealing with Threats 73

Magic tricks are like social engineering attacks 73

MODULE #08 **74**

Review - Bits of security Walkthrough 74

Passwords 74

Which case should we consider - worst case or average case? 74

Identity and Authentication 74

Computer mind model 74

How do we convince the computer that our authentication is correct? 75

Factors of Authentication 75

Multi-Factor Authentication 76

Simple Authentication Protocols 76

Challenge response 76

Authentication vs Authorisation 78

TOCTTOU (Time of check to time of use) error 78

Identity Theft 79

Highlights for 2016: 79

What data do they want? 79

What is done with the data 80

People's Response 80

How to respond 80

Impact on Identity Theft 80

What to do if you are a victim to Identity Theft? 81

Prevention 82

Privacy 82

Stories 82

MODULE #09 **84**

Trust and the Problem of Key Distribution 84

Phishing 84

Non-repudiation 85

Horton Principle 85

Two Approaches: 85

Public Key Infrastructure (PKI): 85

Certificate authority 86

Bruce Schneier: 10 risks with PKIs 87

SSL - Secure Sockets Layer 87

TLS - Transport Layer Security 87

How it works 88

HTTPS - HTTP over SSL or HTTP Secure 88

Perfect Forward Secrecy 88

Address Resolution Protocol and Cache Poisoning 88

Block Modes 89

Electronic Codebook (ECB) 90
Cipher Block Chaining (CBC) 91
Counter (CTR) 92
Pretty Good Privacy (PGP) 93

MODULE #10 95
WannaCrypt Discussion 95
PRE-ATTACK 95
POST-ATTACK 95
Commitments 96
Arbitrariness protocol 96
How do you convince someone you know something in the past? 96
Proving knowledge 96
Zero Knowledge proofs 97
Examples 97
Exam Question Example 97
Maze Example 97
House Burglar Example 98
More on Zero Knowledge Proofs 98
Phishing Attacks 99
Spear phishing 99
Clone phishing 99
Whaling 99
Link manipulation 100
Filter evasion 100
Website forgery 100
Covert redirect 101
Social engineering 101
Phone phishing 101
Other techniques 102
Quantum Computing 102

MODULE #11 102
Trojan 103
Data corruption 103
Incident Response 104
Privacy 104
Other 105

MODULE #12 105
Whistleblowers 106
Exam details 106
Clarification about disaster case study 107
Revision 107

RSA 107
Hash vulnerabilities 108
Bits of security 108
Confusion and diffusion 108
Mandatory access controls 108
Rootkits (from lecture video) 109

CASE STUDIES 109
Module 1 - Deepwater Horizon Disaster 110
Question 110
Module 2 - Houdini 111
Mediums and Channelers 111
THE STRANGE CASE OF "MARGERY" 115
The Medium and the Magician 118
Question 125
Module 3 - Doors on Planes 126
AirNZ Pilots stood down 126
Co-pilot deliberately crashed German Wings flight 127
Pilot opens toilet door with axe 127
AirIndia Pilot locked out of cabin when door jams 128
Question 128
Module 5 - Fukushima 130
Japan split over restart of first nuclear reactor since Fukushima disaster 130
Japan's post-Fukushima nuclear restart plans dealt a blow by court ruling 132
Radiation Is Everywhere, but How to Rate Harm? 134
Is your fear of radiation irrational? 138
Question 145
Module 7 - Johnny Cab 146
Introduction 146
Question 146
Module 10 - Reagan 147
Attempted assassination of Ronald Reagan (Intro) 147
Columbine High School massacre (Intro) 147
Question 148
Module 11 - Disaster 148
How the Boxing Day tsunami unfolded, hour by hour 150
Question 151
Earthquake 151
Tropical Cyclone 152

Extended Presentations 153
Lock Picking 153
Smashing the Stack 153

OpSec 154
VPNs 154
TOR 154
Format Strings 154
Padding Oracle Attack (PKCS7) 155
Chain Block Cipher (CBC) 155
Padding 156
How the attack works 156
How to stop it 157
Additional Resources **159**
Sun Tzu - The Art of War (Summary) 159
DEFINITIONS **161**

MODULE #01

Security engineering - what is security engineering?

"It's ephemeral and illusive" - Richard
! Key problem ! - Why are we unable to write secure software?

- Bridge example and comparison to civil engineering
    - We can build bridges and buildings that won't fall over, and we trust bridges
    - But, we still can't make programs that are bug/error free
- Security engineering is the art and science of managing and controlling errors.
- Mental model: Errors are our "friction", and as complexity increases the friction increases cubically.

The asymmetry between attackers and defenders.

- *Defenders have to win every battle. Attackers only have to win one battle.*
- The idea of the weakest link.
    - Your defence is only as strong as the weakest point. The front door is often made very strong and robust to attacks, but the program may be compromised by other methods of entry.
- To be an effective defender, we have to learn how to think as an attacker, and to know who our attacker is.
- The example Richard used was going to an exercise where he took a class to a building on campus and looking at the physical safety measures. Asking the students first to take a note of the defences, and then challenging them to get in. At first that seemed impossible as the students were really focused on the defence, but changing the mindset to that of a possible attacker. They quickly found a way in (for example by a back door, tailgating etc)
- Suggested reading: Art of War - Sun Tzu
- In spec VS out of spec.
    - A program might be secure and safe when used in spec (as it is meant to be used), but an attacker is trying to force the program to operate out of spec.
- Be sceptical

Digression: Algorithmic verification

- Mathematical proofs of a program's functions.
- Early work done by Dijkstra - Dijkstra's algorithm: finding shortest paths between nodes in a graph (represents e.g. road networks)
- Might be too complex of a task to be successfully applied to real world applications

History of hacking

- Parallels to the history of the development of life. Slow and simple at first, and then a sudden explosion of complexity and specialisation. (with the advent of O_2 in the biological domain, and Microsoft money in the it security one)
- Phreaking on the phone lines in the 1970's with Captain Crunch whistles.
- Example of the problems with having your control signals in line with the user data/input
- Not given a lot of attention in the 80's and 90's. The age of the basement dwellers? ;)
- Explosion in the 2000's. The age of the lone nerd is over. Hacking is now a business conducted by professionals working teams. (and services are sold on a marketplace).

Security Flaw Types

- **Inband -** When the data and control is in the same band. Other than the telecommunication example (Captain Crunch, above), WEP (Wired Equivalent Privacy) security was inband (provides confidentiality). Although was exploited in many ways, one way Richard explained was being able to control the address that the internet packets are delivered to by modifying the IP address. Hence, the decrypt message can be sent straight to you, rather than trying to the decryption yourself. *Always separate data from control stream, prevent users from accessing the control stream.*
- **Complexity -** As described above, when a system becomes too complex, it is prone to errors. Computer programs are built upon layers, upon layers of code that not one sole individual has created or understands completely. Hence, it is very likely that there are mistakes between the joins and unaccounted for inputs that can be taken advantage of. *Where there is complexity, there are vulnerabilities.*
- **In Specification / Out of Specification -** When people write/test applications they focus on the system while it is "in spec". However, someone looking to exploit it will do so "out of spec" - where there are bugs, etc. Hence it is important to consider how a system will behave when "out of spec" or when used in unintended ways. *Don't look at the things that work, look at the things that do not.*
- **Trust -** Humans are trusting by nature. We like to see the good in people (well at least we do). But this can make people easily exploitable. Some of the easiest hacks are just by making people give you too much information and without much technical know how, you're in.

- **Zero Day Exploit -** An exploit that uses a vulnerability in a program that is not yet recognised by the developers or owners of the program.
- **Security by obscurity -** Hoping to confuse people by making the workings of a program obscure is just a facade of security. As soon as an attacker decodes the mess, then the whole thing was pointless. It would also make the code harder to fix.
- **Spear Phishing Attack -** A Phishing attack (pretending to be someone else, usually an authority using email to bait you to click an attachment or disclose information) that is targeting one person specifically.

Crypto Literacy

- **Cryptographic Primitives** - Well established low-level cryptographic algorithms: ciphers, hashes, RNGs, steganography, key generation, etc.
- **Kerckhoffs Principle** - A cryptosystem should be secure even if everything about it, except the key, is public knowledge. Claude Shannon later said that we should assume the enemy will gain full familiarity with them immediately. This combats ‘security by obscurity’.

MODULE #02

Recon

Recon is about gathering information about your target through research and investigations on how they work and operate, to gather data that may be useful later on, such as through social engineering.

Active vs Passive

- **Active** - engaging with the targeted system (such that you could be detected) to gather information about vulnerabilities. Often more effective, but more detectable.
    - Methods used can be seen, traced and may trigger warning systems
    - e.g. sending packets, network requests, emails, analysing header information, scanning for open ports
- **Passive** - collecting information without engaging with the targeted system. Much harder to detect.
    - e.g. whois / reverse DNS lookup, using cloaking/privacy services, spoofing, fake ID, visiting a website like any other user.

Dumpster diving

- Technique used to retrieve information that can be used to attack the target
- e.g. look through trash for access codes, passwords written on paper, Go through someone's trash

Shredding paper

- Burning paper doesn’t to a perfect job
- Shredding can be put back together
- Best methods involve flash paper or destroying only the sensitive information through methods like eating it.

Google disposal

- Google disposes of data by wiping and shredding drives, memory cards etc
- We don’t have to go as far as destroying our data as our information may not be as important as Google.

HOMEWORK: Carry out a recon of one of the following types. Log your progress, report on your findings and reflect on what you have learned about recon.
- shred: reconstruct a shredded paper
- dumpster
- online passive

The problem of security

- **Complexity** - If something is very complex, then it leads to confusion, and then mistakes from misunderstanding.
- **Asymmetry** - easy to attack, hard to defend
- **Weakest link** - If a system is only as strong as weakest link, then only that single link can lead to the entire system failing. (Single point of failure)
- **Hubris** - Thinking like a defender
- **Abuse of trust**
    - People are willing to give out information if they trust the person they are giving it to.
    - Trusting things that shouldn't be trusted.
    - Leads to Social Engineering.
- **Kerckhoffs principle** - A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.
    - E.g. RSA, even if you know it very well, you won't be able to crack it.
    - Formulated by Claude Shannon as one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them (Shannon's Maxim)
    - Combats 'security by obscurity'
- **Human weakness**, typically the weakest link in a system.
- M&Ms - **Single point of failure**:
    - Soft centre, hard shell
    - A lot of organisations are experiencing failures (breaches) from the inside, but they focus only on the outside.
    - ***The basis of a Trojan attack:*** a trusted party enters a system to break it from the inside out.
- **Reliance on secrets is a failure point.**
    - Secrets are very prone to be told or leaked.
    - Assume the attacker knows the system
- **Out of spec**
    - Hackers delight - whatever you imagine it is true
    - If you only ever build your system to follow the spec, it will break as soon as someone goes out of spec.
- **Mixing data and control**

How do we build a secure system?

- Log in your own eye:
    - You are never any good at assessing how good your own system is.
    - Get it checked, have another people check your system.
    - Get more people independent to your company/product to check it.
- Sun Tzu - win without battle
    - "*A poor general goes into battle and wants to win. A good general plans how he is going to win without going to battle.*"
- Process
- Don't rely on obscurity - Schneier points out it is brittle
    - Steganography - the existence of the message is hidden. Once somebody knows a message is there somewhere, they can usually find it.
      The problem is that the secret is too big. Keep the confidentiality small (such as a key).
- Auguste Kerckhoff's principles
    1. The system must be practically, if not mathematically, indecipherable;
    2. It should not require secrecy, and it should not be a problem if it falls into enemy hands;
    3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;
    4. It must be applicable to telegraph communications;
    5. It must be portable, and should not require several persons to handle or operate;
    6. Lastly, given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.
- Defense in depth
    - Multi-layer security, no single points of failure
- Security by design
    - e.g. If the head of security dies, there is a second person who can easily take over.
    - A graceful failure - if a system is going to fail it should fail slowly and allow time to detect the failure and fix the issue.
- Understand assets
    - e.g. the main asset of a library is its books
- Constantly seek for vulnerabilities - evolve
- Anticipate threats
    - Nature: (the actions they do)
    - Source: (who does them) "threat model"
- Analytic approach to Risk
- Prevention, Detection & Response
- Users
- Policy

Engineering Approach

- Design - what is the purpose? Assets / Cost.
    - Tradeoff with undesirable consequences
- Critical, Sceptical
- Listen to your gut - But distrust it.
- Weakest Link
    - Human Factor
    - Brute Force Codes
- Defence In Depth
- Graceful Failure
- Wrong Enemy
    - Threat Model
- Protecting the wrong thing
    - Enumerate/Be Systematic
- Constant
    - Test / Policy
    - Gather Data

Type I and Type II Errors

Reality / Test	Test Positive	Test Negative
Actually Positive	Correct (True Positive)	**Type 2 ERROR** (False Negative)
Actually Negative	**Type 1 ERROR** (False Positive)	Correct (True Negative)

"What you want vs what you get" or Truth vs System results

- There are ALWAYS unintended consequences - it is human nature to be blind to
- In most cases, "minimising" error just moves the error from one bucket to the other rather than minimising it overall.
    - e.g. Increasing sensitivity of cancer screenings means many more false positives, though less false negatives
    - The degree to which this occurs is reliant on Bayes' principle
- Examples:
    - Refugees
    - Jail
    - Automatic Weapon Systems on Drones
    - Alarms - Alarm sounds when there's no incident vs alarm is silent when there is
    - Criminals - an innocent is charged vs a guilty person walks free

- Type I: There is no wolf- people interpret it as “there is a wolf”, where there isn’t a wolf. *There is NO problem, but people think there IS a problem.*
- Type II: There is a wolf - people believe “there is no wolf” and do nothing. *There IS a problem but people think there ISN’t a problem.*

Protocols - CIA

The CIA principle is one that says that we can create a secure system by incorporating the 3 following characteristics:

- **Confidentiality** - People can interact with it and get nothing. We don't get confidentiality because it’s impossible, but we can make it difficult and time consuming by encryption. E.g. The plaintext is invisible until recipient decrypts it.
- **Integrity** - Stop messages from being tampered or changed. One way we do this is by hashing (Such as a HMAC). We verify that the message has not been changed in transmission.
- **Authenticity** - Checking that the messages really came from where they say they do, often through a secret key.

Examples:

1. **Confidentiality**
   - Cryptography
   - Encryption
     - Encryption serves this purpose well because confidentiality is not just about unlocking the door for your mom, it's also about making sure that if someone acts as your mother, they can't get in the house
     - The above alludes to a Man-in-the-middle attack
2. **Integrity**
   - Here we want to check that if we send a message, it arrives untampered. It seems like it may be easy to do but think how it's possible given a man-in-the-middle.
     - Here we see the use of MAC's
3. **Authenticity**
   - How do we verify that someone hasn't intercepted our message? Here we see a relevant use of AES
   - Challenge responses?
   - MAC, HMAC, SKID

Note: **Availability**

- Having information available at the right time. There is no use if the information is unavailable at the time it is needed - DDOS attacks, power outages, natural disasters, etc. To combat this - backup, redundancy, off site location to restore services.

Cryptographic Primitives

Crypto-primitives are like lego, the building block of every protocol. More formally, they are well-established, low-level cryptographic algorithms that are frequently used to build cryptographic protocols for computer security systems. You put different ones together to make a cryptographic protocol. Because of this, cryptographic primitives are designed to do one very specific task in a highly reliable fashion.

Some crypto-primitives:

- **Substitution**
- **Transposition**
- **Split/Concatenation**
    - Splitting bit string and concatenating them (adding them)
- **Bit-by-bit operation**
    - Doing a bit by bit operation on data
        - XOR (most used)
        - AND, OR, NAND, etc..
- **Hash functions**
- **Steganography** - Hiding data in plain sight (e.g. in an image)
- **Encryption**
- **Digital signatures**
- **Cryptographically secure pseudorandom number generators**
- **MAC/HMAC**

Properties of Cryptographic Primitives

Properties	Cryptographic Primitives			
	Encryption	**Hash**	**MAC**	**Digital Signature**
Confidentiality	Yes ✓	No ✗	No ✗	No ✗
Integrity	No ✗	Sometimes ?	Yes ✓	Yes ✓
Authentication	No ✗	No ✗	Yes ✓	Yes ✓
Non-repudiation	No ✗	No ✗	Sometimes ?	Yes ✓

Non-repudiation: The assurance that someone cannot deny something. I.e. If a message has the correct digital signature it must’ve been from the person whether they accept it or not.

Jargon

- **Cryptography**: science of securing data.
- **Cryptanalysis**: science of analysing and breaking encrypted data.
- **Cryptology**: Embraces both cryptography and cryptanalysis.
- **Ciphertext**: Encrypted message
- **Plaintext**: Encrypted message
- **Ciphers**: Cryptographic algorithms, mathematical functions used in the process of the encryption and decryption of data.
- **Encryption and decryption**: Encryption is the process of converting a plaintext message, into ciphertext; Decryption is the reverse process. Specifically, encryption refers to algorithmic schemes that encode plaintext into a cyphertext, providing privacy.
- **Code vs Cipher**
- **Key** is secret compression
- Typically the receiver of the encrypted text uses a "key" to decrypt the message, returning it to its original plain text form.
- A cryptographic algorithm works in combination with a key — a word, number, or phrase — to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys.
- What does it mean to **break** a cipher? - To be able to figure out the plaintext without the need of the key.

Coding practices

Defensive Programming is an approach to improve software and source code in terms of the following:

1. General Quality to reduce the number of software bugs and problems.
2. Making the source code comprehensible, avoiding errors surrounding complexity.

Making the software behave in a predictable manner despite unexpected inputs or user actions.

Bits of Security 

- A rough measure of how much work a task requires.
- It is reasonably independent of assumptions (i.e. if different machines take different amounts of time to complete a task, talking about bits allows us to generalise the time (the log of the number of operations). This gives a more general and rough idea of the amount of work).
    - E.g. if it takes 1000 operations on one machine, and 10 000 on another, this is only a difference of around 4 ‘bits’ of work. (i.e. 2^10 = ~1000, 2^14 = ~10 000). Hence the ‘bits of work’ is a generalisation.
- Exploiting space / time tradeoff can roughly halve the effective number of bits.

- Exponential Growth: Not linear, **squared**. Not doubled!
    - Neapolitan Chess & Rice story.
- 20 bits of work is within the second-minute time range.
- **128 bits** of work is a reasonably large amount of work that would make a system safe i.e. a single hacker couldn't brute force something requiring this amount of work.
- *Worst vs Average case* **-** not really different, probably only by one bit.
- *Worst vs Best case* **-** judge based on the context of the question.
    - If you're the attacker, you want to know the worst case.
    - If you're the defender, you want to know the average case.

Table 7.1: Minimum symmetric key-size in bits for various attackers.

Attacker	Budget	Hardware	Min security
"Hacker"	0	PC	58
	< $400	PC(s)/FPGA	63
	0	"Malware"	77
Small organization	$10k	PC(s)/FPGA	69
Medium organization	$300k	FPGA/ASIC	69
Large organization	$10M	FPGA/ASIC	78
Intelligence agency	$300M	ASIC	84

Worked Example

- Find which of the 54 people has the Easter egg.
- This requires 6 bits of security, since 2^6 = 64 is the closest power of 2 which is equal to or greater than 54.
    - On average, it only takes half the amount, so 5 bits.
- How about if we have 1 million people?
- 20 bits of security since 2^20 ~= 10^6
    - Remember 2^10 = 10^3 so 2^20 = 10^6
- Another way of doing it is to calculate the $ceiling(log_2(n))$

Ciphers

- English Letter Frequency: **etaoin shrdl cumwfgypbvkjxqz**
    - Lack of entropy in English can be exploited to identify patterns in the data.
- Steganography - hiding a secret message within an ordinary message in plain sight.
- Substitution
    - A → O, B → N, C → P, etc.
    - Cryptograms (every letter represents another)
    - To make it more secure you can use
        - Dynamic substitution

                - Make the first occurrence of a letter, say ‘e’ different from the second
                - Hence the first ‘e’ is substituted for an ‘a’ and the second occurrence is substituted with a ‘r’, and third ‘q’ then back to ‘a’
            - One to many
                - ‘E’ could be either substituted with ‘W’, ‘M’ or ‘O’, randomly selected during the making of the encrypted text
        - This eliminates the use of letter frequency and other techniques
- Transposition
    - Positions of plaintext are shifted systematically. E.g.: rail fence cipher
    - Changing the order the characters appear
    - ‘ABCD’ ----transposed---> ‘CDAB’
    - This is not random and usually requires a key to transpose and de-transpose
- Entropy + order / redundancy
- Bigrams: eg Playfair - encrypts pairs instead of single letters.

Old Codes

Substitution Cipher

The layman explanation of a substitution cipher - where we replace one occurrence of a letter with a ciphertext character:

- You may be familiar with the famous ROT 13. However, the methods definitely increase in range of complexity
- Caesar cipher also called a Mono-Alphabetic Substitution cipher
- This is one of the simplest Ciphers. It was effective in Ancient Rome, but is weak because it a) relies on a shared secret b) is easy to brute force (via frequency)
- To rectify brute-forcing:
    - Different shifts, e.g. letter "e" shifts a different number of times
        - Called Poly-alphabetic Substitution cipher.
        - Different "alphabet" per letter for a sequence of letters(n) and then repeat alphabets. In this case, you would need n shared secrets.
        - Communicate using BED (Shift by 2,5,4) - Vigenere cipher
        - Solved using frequency analysis. If still no joy you can systematically remove every nth letter and doing a frequency analysis.
- Other examples:
    - Vigenere Cipher - this one is worth looking at. It takes a word like hello, and performs some operation like:
    - letter + wordletter mod 26 = output
    - If we wanted to encode the word yellow first it would take y:
        - y + h mod 26 = output
        - and repeats
    - A Vigenère cipher is an example of a polyalphabetic substitution cipher.

Transposition Cipher

In a transposition cipher, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged.

Examples of transposition ciphers:

- Rail fence cipher
- Columnar transposition
  https://en.wikipedia.org/wiki/Transposition_cipher#Route_cipher

Bigrams: eg Playfair

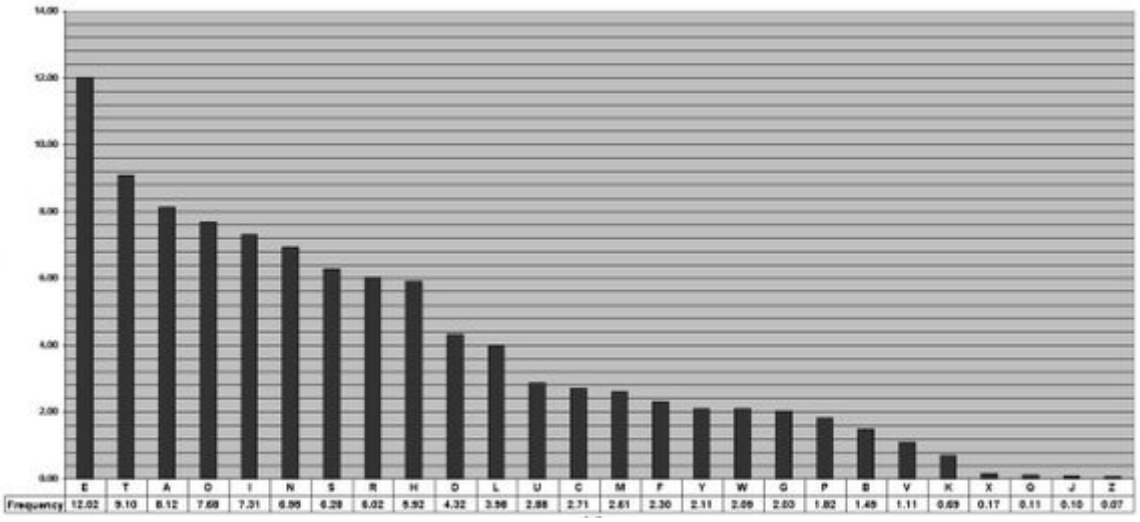
- A type of substitution cipher whereby pairs of letters in the plain text are substituted with another pair of letters generated by a 5 by 5 alphabet table diagram.
- Refer to Playfair Cipher Explained by Kenny Lam on Youtube (4 min video) for more details.
  - https://youtu.be/quKhvu2tPy8
- Another video to explain the Playfair Cipher - if you find the above too fast-paced
  - https://www.youtube.com/watch?v=3c1PE5vPSRo

Steganography - hiding a secret message within an ordinary message

- e.g. Writing secret messages directly on the wooden panel of a wax tablet, then covering it with the beeswax surface
- There may not be any steganography on the mooc
- E.g. Tattoo message hidden on a slave's bald head. Then let his hair grow so it covers the message while he carries a fake message by hand. If the enemy captures him, they will only see the fake message but not the true hidden message.
- Once someone solves the steganography, they will know the code right away. So we need another layer on top such as substitution.

Solving a Cipher

- Assess the frequency distribution - this helps to figure out if it's a substitution cipher or a transposition cipher
- Dictionary in /usr/share/dict/words
- If the frequency distribution looks roughly like this:



- Then this is likely a transposition cipher
- However, if it follows this distribution but the letters are not ETAOIN... but rather some other letters - you may be looking at a substitution cipher

Cipher Handbook

- **Coincidence** Index = Frequency ÷ |CipherText| × 26
    - Coincidence Index of common languages
        - English : 1.73
        - Russian : 1.76
        - Italian : 1.94
        - Portuguese : 1.94
        - Spanish : 1.94
        - French : 2.02
        - German : 2.05
        - Usually a Vigenere ciphertext will have a CI between 0.4 and 0.5
- **Twincidence** Index = Doubles Count ÷ |Corpus Letters| × 26
- **Benford's Law**: The likelihood of the 1st digit (d) is proportional to… log(1+1/d)
    - The law states that in many naturally occurring collections of numbers, the leading significant digit is likely to be small.
    - Where d is the first digit of the number

d	P(d)
1	30.1%
2	17.6%
3	12.5%
4	9.7%

5	7.9%
6	6.7%
7	5.8%
8	5.1%
9	4.6%

Frequencies of the letters in the English language

E	12.51
T	9.25
A	8.04
O	7.6
I	7.26
N	7.09
S	6.54
R	6.12
H	5.49
L	4.14
D	3.99
C	3.06
U	2.71
M	2.53
F	2.3
P	2
G	1.96
W	1.92
Y	1.73
B	1.54
V	0.99
K	0.67
X	0.19
J	0.16
Q	0.11
Z	0.09

The most common first letter in a word in order of frequency

T, O, A, W, B, C, D, S, F, M, R, H, I, Y, E, G, L, N, O, U, J, K

The most common second letter in a word in order of frequency

H, O, E, I, A, U, N, R, T

The most common third letter in a word in order of frequency

E, S, A, R, N, I

The most common last letter in a word in order of frequency

E, S, T, D, N, R, Y, F, L, O, G, H, A, K, M, P, U, W

More than half of all words end with

E ,T, D, S

Letters most likely to follow E in order of frequency

R,S,N,D

The most common digraphs on order of frequency

TH, HE, AN, IN, ER, ON, RE, ED, ND, HA, AT, EN, ES, OF, NT, EA, TI, TO, IO, LE, IS, OU, AR, AS, DE, RT, VE

The most common trigraphs in order of frequency

THE, AND, THA, ENT, ION, TIO, FOR, NDE, HAS, NCE, TIS, OFT, MEN

The most common double letters in order of frequency

SS, EE, TT, FF, LL, MM, OO

The most common two-letter words in order of frequency

of, to, in, it, is, be, as, at, so, we, he, by, or, on, do, if, me, my, up, an, go, no, us, am

The most common three-letter words in order of frequency

the, and, for, are, but, not, you, all, any, can, had, her, was, one, our, out, day, get, has, him, his, how, man, new, now, old, see, two, way, who, boy, did, its, let, put, say, she, too, use

The most common four-letter words in order of frequency

that, with, have, this, will, your, from, they, know, want, been, good, much, some, time, very, when, come, here, just, like, long, make, many, more, only, over, such, take, than, them, well, were

The most commonly used words in the English language in order of frequency

the, of, and, to, in, a, is, that, be, it, by, are, for, was, as, he, with, on, his, at, which, but, from, has, this, will, one, have, not, were, or, all, their, an, I, there, been, many, more, so, when, had, may, today, who, would, time, we, about, after, dollars, if, my, other, some, them, being, its, no, only, over, very, you, into, most, than, they, day, even, made, out, first, great, must, these, can, days, every, found, general, her, here, last, new, now, people, public, said, since, still, such, through, under, up, war, well, where, while, years, before, between, country, debts, good, him, interest, large, like, make, our, take, upon, what

	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
W	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

MODULE #03

Risk

- Risk is invisible, only the outcomes are visible
- Risks are always bad no matter the outcome --> a good or bad outcome is simply left to chance eg. Living near volcano
- In the security world, past data is likely not valid, or events/breaches have not happened before so data is non-existent. This impacts our ability to judge risk, often with severe or fatal consequences.
- Two key reactions to low probability, high impact risk (humans are the weakest link):
    - OMG! That's terrible! Invest all resources and time and forget other risks
    - Naaah, never gonna happen
- Humans are bad at assessing these low probability events because we rarely witness them, and it's hard to put a price on them.
- Contemplating risk example - There are 2 computer repair stores. One did everything very precisely and carefully, whilst the other quickly and dangerously flung the computer around to repair it. However, the customer doesn't always see these inner workings. What they do see is $20, $50 .... savings. They may see an occasional bad review, but if the majority of repairs work at the risky shop, it may still be the most appealing. But now take away the curtains, it then becomes a question of **putting a price on risk.**

Approaches to dealing with risks

1. **Prevention:** Elimination of the threat such that the undesirable event is guaranteed not to occur. Inherent safety prevents undesired events. E.g. removing the bolt and bullets from a rifle to prevent it from accidentally firing.
2. **Limit:** In situations which the threat could not be eliminated, mechanisms are implemented to minimize the impact resulting from the event (fault tolerance) or reduce the likelihood of it occurring (probabilistic safety). E.g. a castle with concentric walls. Even if one wall is breached, only a limited portion of the castle is compromised.
3. **Passing the risk to a 3rd party:** This involves in making another person/entity the bearer of the risk. Generally taking out an insurance policy is used minimize or negate financial loss in an event of a failure.
4. **Wear** the risk and accept that it will happen.

Keys /

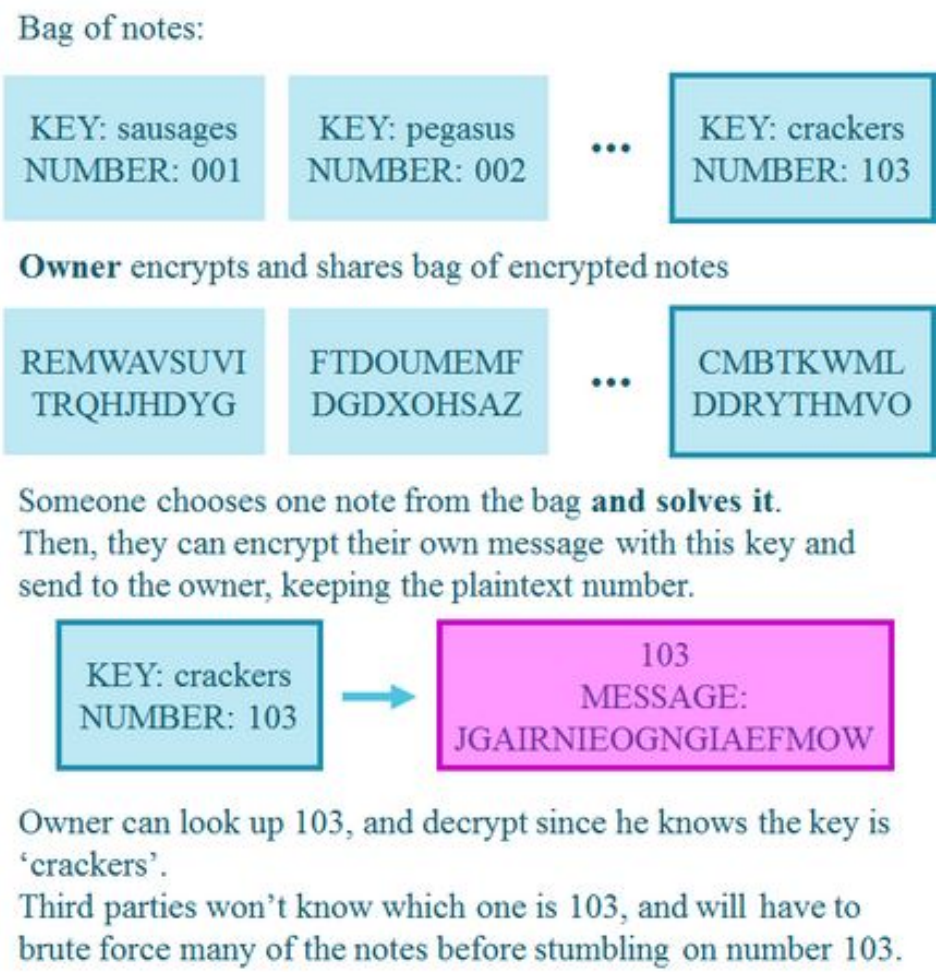
- An abundance of people and keys is hard to manage and distribute securely

- Public/Private keys have and asymmetric nature
    - one public key - anybody can see it and encrypt whatever they want
        - the resulting message can only be decrypted with the corresponding private key
        - prevents others from reading the message (confidentiality)
        - applications include: encryption, digital signatures
    - one private key - is usually kept as a secret
        - It can decrypt anything encrypted with the public key
        - It can also “encrypt” (or more formally, sign) messages such that the public key can decrypt and read them and thus the public can authenticate the sender.
        - Can be used to “sign” something

Merkle's Puzzles

1. Merkle generates a large Bag of brute forceable cipher texts each with a unique message number and a unique key encoded within the message. The creator knows all.
2. Someone has only to brute force/crack one cipher to read its message and gain the message number and its key.
3. The person then can reply stating it’s number and then encrypting the rest of the message using the key.
4. Merkle can then decrypt by selecting the corresponding key using the given number.

Any third party would have to brute force/crack the code of every other message until they crack a message with the corresponding number to be able to understand/crack said reply.
On average, the third party would have to crack least 1/2 of all messages to find it.
This relies on the asymmetry for security--> it would take much longer time to decode every other message, than it would to send the ciphertext.
An attacker would require O(n*t) time to brute force all the messages. (where n is the number of messages and t is the time to bruteforce 1 message)
But a quadratic barrier is not a big enough restraint.



One Way Function

- A cryptographic function that encrypts a message easily with a key, but makes it very hard to obtain the original message given the encrypted message without the key is known as a trap-door function.
    - An example of this is factoring multiples. It is easy to multiply them but extremely difficult to factor them.
- NP-Complete problems are a class of problems that are very hard to solve. We use these for generating trap-door functions.
    - E.g. The discrete log problem, $g^k \bmod n$
    - We can give away g, n and ($g^k \bmod n$) but it is very difficult to work out what k is.

Math Review

Exponent Laws

$(x^a)^b = x^{ab} = (x^b)^a$

Modular Arithmetic --> take the remainder

$13 \equiv 1(mod\ 3)$ Where $13 \div 3 = 4$ ***remainder 1***

$x^y \equiv 1347192834\ (mod\ z)$ --> y is hard to work out

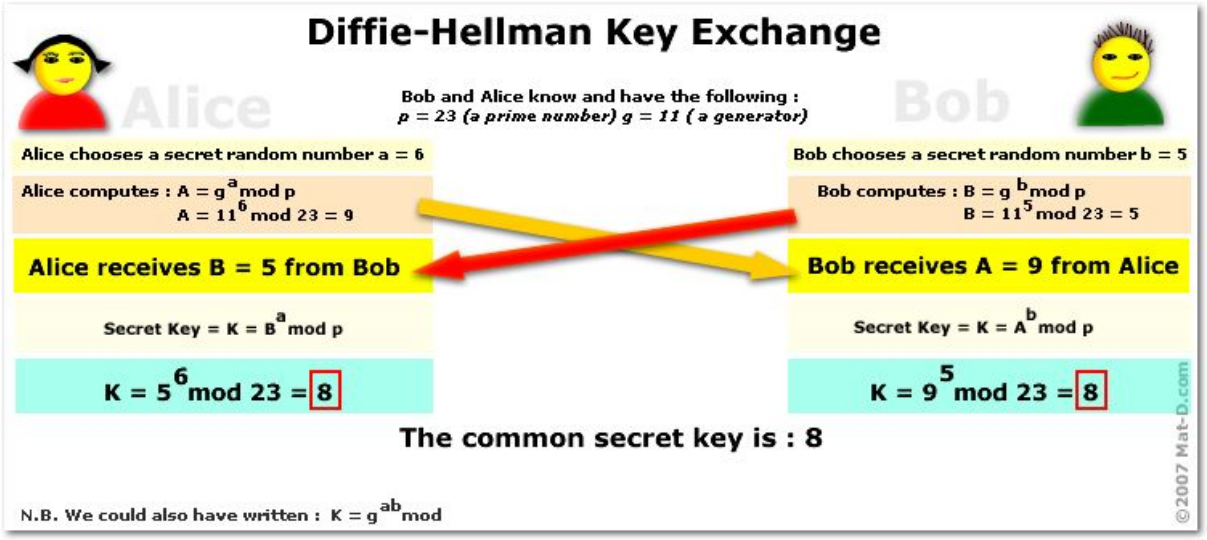
Diffie Hellman Key Exchange

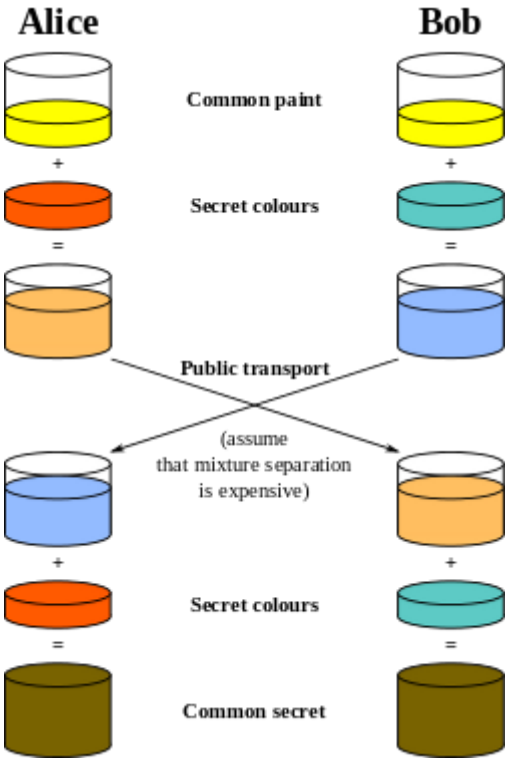
Is a key-exchange algorithm that allows two parties to agree on a shared key without having met before. This attack makes it impossible for eavesdroppers (observing traffic, not changing it) to know anything that's being shared, however it can be man in the middle'd.

- It provides **confidentiality** because discrete logs are difficult to work backwards from to find the keys a or b.
- On top of all this, neither party has to know the other's secret number, so they can both keep it for future conversations with other parties.
- All ingredients are shared publicly (so it can take place over an unsecure channel)
- Gets over the problem of having to share keys in the first place
- Symmetric crypto system
- Has a good **confidence level** because it ties the algorithm to a known NP-complete problem (discrete logs).
    - We can be confident that the message will not be broken because we know (and many people have tried and failed) that discrete logs have no easy way for working backwards (yet).
- Some of the problems include forward secrecy, once one value has been cracked, then so can many others.
- It can also be subject to a MiTM attack.

How it works

- Alice and Bob publicly decide on a base g and mod m
- Alice selects secret value a.
- Bob selects secret value b. (both these values can't be larger than m)
- Alice sends g^a (mod m) to Bob.
- Bob sends g^b (mod m) to Alice.
- Both compute shared secret g^ab (mod m) since g^ab = (g^a)^b.
- Shared secret can be used as symmetric key.





RSA

- Uses a public key, which is a one-way function, to encrypt messages (shared with everyone)
- Uses a private key, which only the recipient knows, to decrypt a message
- Post office box example:
    - Encrypt a message using public key function and deliver it
    - Recipient uses their key to open the PO box and decrypt the message

How it Works

Bob has a message that he converts into a number using a padding scheme, call this **M**. Alice generates her public (**N**, **E**), and private keys (**P1**, **P2**, **D**), as follows:

1. She generates 2 large (around 150 digits) random prime numbers of similar size **P1**, and **P2**, then multiplies them together to get a composite number **P1***P2** = **N**.
2. She calculates Phi(**N**) as (**P2** - 1)*(**P2** - 1), which is a one-way function, since it is only easily done if you know the prime factorisation of **N**.
3. She picks some small public exponent **E**, with the condition that its an odd number, that is co-prime to Phi(**N**) such that gcd(**E,** Phi(**N**)) = 1.
4. She then calculates d such that **D***E = 1 mod Phi(**N**)
5. Alice then hides everything, except the values **N**, and **E**, which are her public key.

- Bob then encrypts his message (**M**) using the following formula: $\mathbf{M}^{\mathbf{E}}$ mod(**N**) = **C**. He then sends his encrypted message **C**, back to Alice.
- Alice uses her private key **D**, to decrypt the message using the following formula: $\mathbf{C}^{\mathbf{D}}$ MOD **N** = **M**, which is Bob's original message **M**!
- Notice that Eve (anyone listening in) can only find **D** if they knew the prime factorisation of **N**. If **N** is large enough, Alice can be sure this could take hundreds of years, even with a network of the most powerful computers.
- Encrypt a number by just raising it by a power and modding it
- We choose the numbers to be co-prime numbers to prevent collisions
- We choose large primes to make it harder to crack
- We raise the encrypted number to a decrypt number to get the original number
- To calculate the decrypt key you need the original two numbers - it would take too long to brute force

Another Explanation

- We generate a key pair (n, e) and d such that (m^e mod n = c) and (c^d mod n = m)
- Our public key is (n, e) and private key is (n ,d)
- Someone who wants to send us a message takes the message m and our public key (n, e) to generate an encrypted message: m^e mod n = (encrypted message)
- We perform (encrypted message)^d mod n = m, the original message
- **How to generate key pair**
    - Choose 2 large prime numbers p, q
    - Compute
        - n = pq
        - phi(n) or t = (p-1)(q-1)
    - Choose e where e < n that has no common factors with t (co-prime)
    - Choose d such that e*d mod t = 1
    - Public key is (n, e)
    - Private key is (n, d)
- **Parameter conditions**

- **p, q** Prime, preferably 1024 bits long each
- **e** e < n
- **phi(n) or t** No common factors with e or d (co-prime)
- **d** ed mod z = 1 (product ed is divisible by t)

Encrypt with public key

- (message)^e mod n = (encrypted message)

Decrypt with private key

- (encrypted message)^d mod n = (message)

Worked examples

Example 1

1. We have an encryption key 7 and a number n = 77v
2. Find p and q which is 77 = p * q. Hence p = 7 and q = 11
3. Find phi(n) = (p-1) *(q-1) = 6* * 10 = 60
4. Now use phi(n) to find a decryption key such that it solves this equation for d: e*d mod phi(n) = 1. Sub values in: 7 * d mod 60 = 1.
5. We find d = 43 solves this equation.
6. Let's test it back into our original encryption algorithm. So let's choose a number to encrypt - 7.
7. Encrypt 7 = 7 * 7 mod 77 = 28. Encrypted number is 28.
8. Now let's decrypt it with the key! So 28 * 43 mod 77 = 7. This is our original number!

Example 2

Choose p = 3 and q = 11

1. Compute n = p * q = 3 * 11 = 33
2. Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
3. Choose e such that 1 < e < φ(n) and e and φ (n) are coprime. Let e = 7
4. Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
5. Public key is (e, n) => (7, 33)
6. Private key is (d, n) => (3, 33)
7. The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
8. The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

Encryption Function: x^k mod p

1. Let prime p be $7 \times 11 = 77$
2. Let the encryption key k be 7

You can share k = 7 and p = 77

x^7 mod 77

Example:
k = 3
$p_1 = 5$
$p_2 = 11$
Encrypt with x^3 mod 55 − say x = 6
6^3 mod 55 = **51**

Decryption Function: y^n **mod** p

1. Calculate $m = (7 - 1)(11 - 1) = 60$ from the prime numbers, **keep secret**!
2. Let n be the decrypt key where $n \times k \bmod m = 1$ – here n = 43

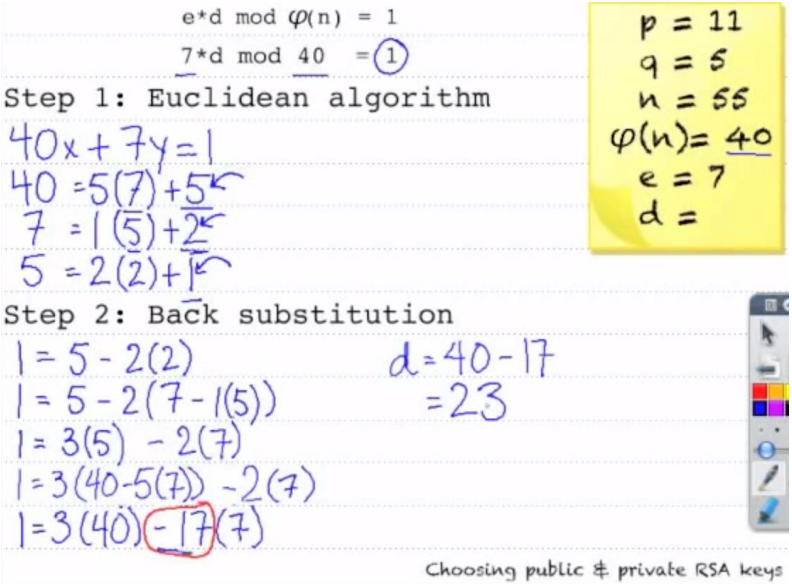
Private: y^{43} mod 77

Alice tells us secretly $m = 4 \times 10 = 40$
k = 3
n is 27 ($27 \times 3 \bmod 40 = 1$)
Decrypt with y^{27} mod 55 − y is 51
51^{27} mod 55 = **6**

Euclid’s Algorithm

If brute forcing seems difficult try Euclidean algorithm.
e*x + phi*y = gcd(e, phi) = 1
e*x === 1 % phi, x = d
so:
e*x + phi*y = 1
phi = k_1*d + r_1
d = k_2*r_2 + r_2

https://youtu.be/kYasb426Yjk



MODULE #04

Human Weakness

- Humans will be the **weakest part** of any cybersecurity system.
    - Rather than recommend technical/hardware advice, to be a good security engineer/advisor you need to understand the weakness of humans.
    - Everything in the news is about human weakness.
- We are utterly flawed in every respect.
    - Ethics: we still act appropriately even if no-one is looking.
    - It can be tempting to do the wrong thing (corruption, acting badly)
    - People in power abusing the trust/power they have.
        - Analytical: what do these people (who do the wrong thing with power) have in common. Why didn't we see these characteristics earlier? BECAUSE IT CAN BE ANYONE
        - There is a constant percentage of tellers/bank employees 'going bad' and doing the wrong thing. And the banks can't work out who it's going to be.
- **Human Weaknesses:**
    - Greed, Temptation, addiction, pleasure-seeking.
        - Money, power, fame pushing people to act irrationally.
    - Fear
        - South Korean Ferry Disaster: Many were not willing to name the faults; living in fear of the company.
    - Laziness
        - A check that should be done.
        - Walking in a straight line even if the path is curved.
        - Skipping protocol checks
    - Pride, ego, narcissism
        - Can stop reflection/criticism of bad behaviour.
        - An elevated human ego can change the perception of reality
        - Leads to hubris -- My system will never fail !
    - Curiosity
        - We'll always press the button
        - Really only bad for cats
    - Anger, Revenge
        - We lose common sense when emotions run high.
        - Revenge to yourself can also be a weakness
    - Trusting, being naive
        - We put too much trust in other people. We have to put trust in some things, otherwise we would spend the whole time checking things.
        - Imagine checking every assumption in code: it would be ridiculous. Programs work by assumptions and trust.
        - Most social engineering exploits trust.

        - Ignorance represents a human weakness. Like poorly trained security staff.
    - Complexity overload
        - When something is too complex/daunting, people become overwhelmed and give up.
    - Desensitization to risk - normalization from environment
        - Likely to agree with others, even if everyone else is wrong.
        - Habitually performing risky actions lessens the perceived threat of the action.
        - Environment conditions could lead to a different perception of reality: snow, fog, rain, etc.
    - Diffusion of responsibility
        - “It’s not my problem”. The bystander effect. You may not notice that you should do something if nobody else is doing anything.
- Most of the famous breaches/attacks have been directly enabled/caused by the **exploitation of human weaknesses**.
- **Costa Concordia Disaster (2012)**
    - The captain fled immediately, but was supposed to evacuate the passengers
    - Much bad practice and corruption leading up to disaster
    - Use security eyes for everything: read about disasters and work out what went wrong, and what are the right things to do at the time. What did people do? What didn’t they do?
- **South Korea Sewol Ferry Disaster (2014)**
    - The captain and crew were among the first to evacuate
    - They made announcements for passengers to stay in their cabins
    - Those who disobeyed the orders survived.
    - No training on how to deal for emergencies. USD$2 budget for safety.
- All these examples: being normalised by what is around them, acting for self-interest or to protect friends rather than general public leading to systemic failure.
    - Need to understand HOW things go wrong in order to prevent this sequence of systemic failure.
- **Rick Rescorla**
    - Head of security for Morgan Stanley (World Trade Centre).
    - Realised the Port Authority were inept, and if any evacuation was necessary, he wasn’t confident that the port authority could carry it out safely.
    - Got someone to analyse the building, and told his bosses that the building was unsafe, and unsuitable.
    - He recommended moving to a different location, but this wasn’t accepted for a while.
    - In the meantime:
        - He trained/drill everybody in how to completely evacuate the building.
    - When the plane crashed into the first building, and it was announced that the second building was safe, Rick immediately picked up a radio and contradicted the order, and saved around 2000 lives by forcing this evacuation.
- **Responses to Human Weakness**

    - Train/drill our responses to human weakness, specially others who are lazy/inept, so that everyone is ready for disaster.
    - Train / drill people to not only be prepared for a cyber attack but to mitigate risks that could lead to an attack.
    - Think about the potential for disaster BEFORE it happens.
    - Policy doesn't solve the problem: you have to train others.
- **Security Theatre**
    - Having large, heavy systems in place that appear secure, but are really just to 'scare off' villains. This is a bad approach to security. E.g.: Airport security control in the US after 9/11.
- Magicians are good at finding our weaknesses
    - Most 'magic' is about psychology, **distraction** and **misdirection**.
    - Watch some magicians, work out how their tricks work.

Examples of human weakness

- Sacked for **cheating** on his travel expenses: Florencio López-de-Silanes **head** of the Institute for **Corporate Governance at Yale**'s School of Management.
- *Before long, we're going to find out what the judge thinks of the government's case that Professor Andrei Shleifer and Jonathan Hay **illegally speculated** in Russian stocks and bonds, even as they directed a US-funded, Harvard-backed project to help the Russian government s**et up honest and transparent capital markets** -- a project whose rules expressly forbid them to invest in the host country.*
- *"TIAA-CREF, a large institutional investor as well as a **prominent governance activist**, is the target of a Securities and Exchange Commission inquiry into a business relationship that its auditors entered into with two of the fund's trustees in 2003. The pair resigned their TIAA-CREF positions Nov. 30. SEC rules bar accounting firms from entering business ventures with their audit clients."* THE WALL STREET JOURNAL January 10, 2005; Page B1
- 2005 September ***Bayou Group** founder Samuel Israel III and CFO Daniel Marino pleaded guilty Thursday to charges that they swindled more than $450 million from investors. Federal prosecutors say that the duo convinced investors to put more than $450 million into Bayou hedge funds and then conspired to lie about the funds' returns and issued phony accounting statements to investors*

Physical Security

- If someone has physical access to your hard drive, then it's game over.
- Precursor to Computer Security: There is no point having the world's most complex and wonderful communication protocol if somebody can just take the hard drive.
- Whoever has physical access wins (more or less).

    - You could try and hack the encryption, or just put a keylogger on the transmission device (microphone, camera, wireless intercept, soldered to keyboard etc.)
- All computer security starts by limiting physical access.
- Recent leaks by CIA: Originally working by physical means (the easiest access method).
- Physical security is also the hardest to secure.
    - Context: Many don't know much about physical security, so when you see it, you are impressed (even if it's not that secure). Once we see one component that seems heavy/tough we give up.
- Tamper Evident vs. Tamper Proof
    - Is it sufficient to make it evident that somebody tampered with it, or does it need to prevent tampering.
    - Ensure something physically it's mapped to the digital mapping, as in serial numbers on hardware. E.g: Swapping barcodes on hardware.
    - Example: ballot boxes and vote counting security - security tags seal ballot boxes but new tags are accessible nearby,
- Keep your eyes open whenever you are in a place that should be secure: watch for physical weaknesses

Hashing

- A hash function is a function that takes a variable length input and produces a fixed length output.
- Hashes look after the **i**ntegrity/(**a**uthentication) of the data.
- C (confidentiality) doesn't really count. It doesn't matter if the data is understood. It just can't be changed.
- A Hashed message can be seen as the fingerprint of the message, the hashed message identifies the message.
- No Secrecy, the function and output can be public knowledge.
- Hashes mean we don't have to store passwords on systems. We can just store the hash of the password and then compare that every time.
    - Dictionary attacks consist of hashing common words for passwords to see if they match with any of the hashed passwords on the system.
    - We can prevent this through salting
        - Consists of pre-append a random number to the front of everyone's password (the number can be public).
        - Even if an attacker has access to the salt values, the attacker now has to try each hash with every other salt, squaring our workload.

Hashing vs Encryption:

- Hashing is irreversible
- Hashing gives out fixed length output - unlike encryption which produces similar length to the original text

- Hashing doesn't need an encryption key, but there do exist hashes which can be encrypted.

Cryptographic Hash Properties

- Just like normal hashes, except there is no correlation between the input and output.
- **Diode property** - you can go one way, but it's very difficult to go the other way.
    - Easy to find the hash given the message, but hard to find the message given the hash.
- **Avalanche effect** - a small change in the message should result in a ~50% change to the hash.
- **Collision resistant** - A proper cryptographic hash, whilst still subject to collisions, should have chance of collision equal to 1 in 2^n where n is the size of hash in bits (e.g. 256-bit hash is a 1 in 2^256 chance of collision)

Hashing Attacks

Preimage attack

- Given a specific hash, a preimage attack tries to find the original message from the corresponding hash value.
- A cryptographic hash should resist a preimage attack, such as by making it very difficult to reverse the hashing process.
- Brute force takes about $O(2^n)$

Second Preimage Attack

- Given a message AND its computed hash, a second preimage attack finds *another* message that has the same hash.
- Resistance to this sort of attack is necessary when the message itself is not a secret but the concern is that no one can produce another message which has the same hash.
- Another way of understanding this is that, say your hash function was weak and only did a sum of all the characters, then you could just change the order of all the characters and get back the same hash value.

Birthday Attack (Attacking the Hash's Collision resistance)

- Can you find two messages that have the same hash?
- In this case the hash is not known
- Based on the Birthday Paradox (a paradox because there is no paradox): given a certain number (min 24) of people in a room, there is >50% chance that at least two people share a birthday. It's counterintuitive: you think it's unlikely, but the number of pairs grows quadratically as the size of the sample increases.

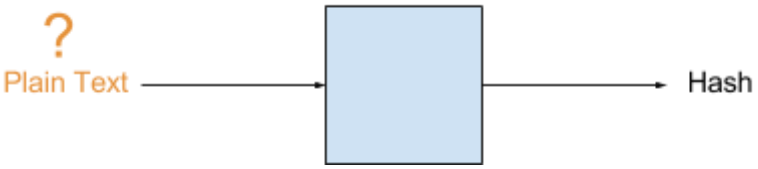
- The chance of finding a collision when computing new hashes increases quadratically, so you only have to check, on average, the square root of the number of possible hashes.
- Collision attacks are bad because a bad message could be verified as a good message, as they would both have the same hash.
- Birthday attack on collisions takes about SQRT(items) on average. ie $O(2^{n/2})$

Hashing Attack Examples

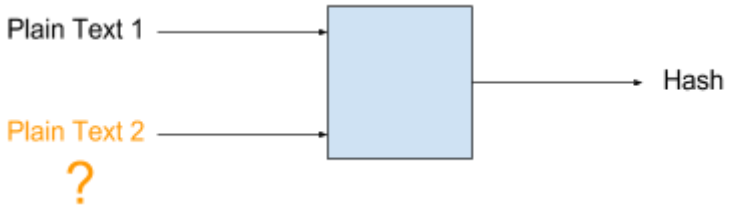
- **First pre-image resistance:** If you were told, “I know someone with this birthday”, then the only way of finding who that person is, is by brute force.
- **Second preimage resistance:** Can you find someone else who has the same birthday as some person? You would have to find his birthday, then ask everyone else for their birthday. Or you could try to find his twin if you wanted to be faster.
- **Collision resistance:** Can you, in the room, find two people with the same birthday? Over time, this process gets easier and easier as we can compare with everyone else we've already established.

Hashing Attacks Pictorially

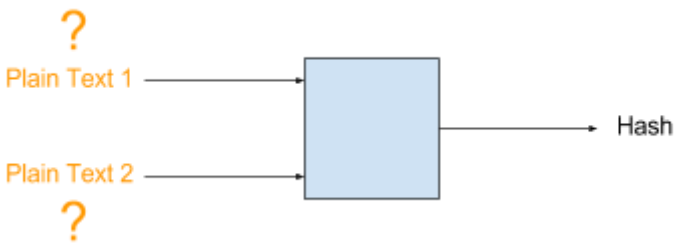
Preimage Attack



Second Preimage Attack



Collision Attack (Birthday Attack)



Hashing Algorithms

- CRC family: Cyclic redundancy check.
- MD5 - too small (easy to brute force) <64 bits. It isn't collision resistant.
- SHA (0, 1, 2) - all co-developed by the NSA. 0, 1 are already broken.
- SHA2 is the industry standard, ranges from 256:128, 512:256
- SHA3 is new and isn't prone to length extension attacks, not made by the NSA.
- "Broken" - once you can attack it faster than brute force.

MAC - Message Authentication Code

- A MAC solves the problem of verifying that the message being sent hasn't been intercepted and changed, or replayed.
    - Both parties agree on a pre-shared secret or key.
    - Each sender then sends the original message plus the hash of the original message and the secret.
        - M = M + H(M + S)
    - The receiver then takes the message, splits it, and follows the same process, checking that the hashes are identical.
- This guarantees that only someone who knew the pre-shared secret could alter the message.

NONCE

- However this doesn't stop replay attacks, as a MitM could just save the message and play it again.
- So we now include a **Nonce** in our message.
    - M = M + N + H(M + S + N)
    - A Nonce is a number that is only used once, this can be a random number, the time of day, a counter, etc.
    - It must change every transaction.

Length Extension Attacks

- Length Extension Attacks can break a MAC by extending the original message. This is a problem because most hashes are rolling, or iterative. (taking one part of the message, doing something, and then taking the next part)
- If you know the hash of the whole phrase, there's nothing to stop you adding something to the end of the message (since the unknown part is only at the beginning), and just updating the hash.
- It's also possible to just dictionary attack the password.
- We prevent this using a HMAC
    - Hmac - puts the hash of the first half at the end, then hash everything again.
    - M = M + H(S + H(S + M))
- *Length Extension Attack*: Many cryptographic hashes are iterative (take one part of

MODULE #05

Vulnerabilities and exploits

Vulnerability - something that has a potential flaw, leaving you weak. A software bug.

Exploit - something that takes advantage of a vulnerability.

- We are still writing code with new and old vulnerabilities. They are so hard to deal with because they are so hard to spot
- It's a game of cat and mouse - the bad guys do something, the good guys pounce, the bad guys have moved, and so on.

Bug Types

Memory *corruption* - allowing changes to memory in areas the programmer was not expecting you to be able to edit. Examples of these include things like variables, stack elements etc. It might be possible for this to be stamped out. Lots of research in this field, maybe in a decade or so, but Richard says other ones will appear to take their place.

Buffer Overflow - Area of memory set aside to store info. It stores a variable amount of information, sorta a temporary storage area. The early version of this was just writing more than the buffer was set up to take. The array would keep writing in memory after the array, and you can overwrite into other variables and so on. You have to be systematic, or careful and lucky to get a useful effect.

Calling functions - You can trick a program into calling different functions by popping something onto the stack and by changing the return address of a function.

Exploits

Buffer Overflow - one of the most common memory corruption attacks. This happens when user input is longer than pre-allocated space. "That array is so big, it will never fill up" - a busy programmer will neglects all the checks and so on. This is dangerous as the input can then overwrite important parts of the program allowing someone to possibly overwriting variables or executing malicious code. An example of what this can do: when a function is called, the stack frame stores function variables as well as the return address. If somehow you manage find the address offset and overwrite a part of the program memory and alter the return address, you can make the program to jump to somewhere else, eg. your own malicious code segment.

Shell code - piece of code that aims to pop a shell (a remote terminal for you into their system), and preferably get root access. You write in your own code for doing something like

popping a shell, then make use of a buffer overflow to insert the code and a return address to call it. The trick for this is finding where to write to.

NOP sled - NOP = no-operation instructions. When you don't know precisely where things are in memory, a NOP sled is effectively a way to widen your landing point. It involves writing a list of instructions that have no effect on the computer, and at the end putting the code that you want implemented. Because nothing happens when the initial instructions are implemented, it doesn't matter precisely what point your code tells the computer to jump to - it will just 'slide' to the end. The simple ones are easily monitored for, so people continuously develop more subtle methods of creating the effect.

Format Strings (printf()) occurs when the submitted data of an input string is evaluated as a command by the application. The attacker can execute code, read the stack, or cause a segmentation fault in the running application, causing new behaviors that could compromise the security or the stability of a system.

Common bugs

Most bugs arise from complexity and human error.

- Signness (being able to have a negative sign) of entry data could allow users to enter negatives, and when we pass that into read, it becomes unsigned, which wraps around to a really big number.
- Missing if braces can result in statements being run when we're not checking for overflows
- 040 in c is octal, not 40 in c
- if we have assignments in if statements, they will always be false.
- In c, when we convert large unsigned numbers into signed values, the beginning bit marks that its negative

Common Vulnerabilities and Exposures (CVE)

National Vulnerability Database is a system that provides a reference-method for publicly known information-security vulnerabilities and exposures.

CVE Number - Common Vulnerabilities and Exposures number. It's like finding an asteroid. Takes the format of CVE-YYYY-NNNN (Y being the year, n being the number)

- Unless you set out specifically what you are defending, it's hard to defend everything and we tend to defend the wrong things.
- The CVE Database is important as it holds companies responsible for vulnerabilities that have been discovered and haven’t been patched yet.
- It also stops VEs from being rediscovered over and over again.

Assets

- Work out what all the things you should be protecting and their relative value to you.
- The issue is often people skip this step because they think they know what they want to protect. There is often some not so obvious asset that when it's lost, you will kick yourself.

Strategies for identifying assets

- Get lots of eyes looking at it, including the people who own the assets.
- Regularly surveying the values of people of the involved in what you are protecting.
- Tease information out of your clients, humans are poor at regurgitating.
- Everyone suggest ideas and then everyone else criticises it (we are good critics)
- Periodically revise assets - Once we identify and asset we need to keep expanding the list.
- Invest authority power into the process.
- Look at different areas in different ways
- A very common asset that is hidden is reputation, since it's not tangible.
- Assets come down into two categories:
    - **Tangible assets** - easily given value (usually something physical)
        - E.g. Jewellery, money, etc.
    - **Intangible assets** - can't be easily and objectively valued
        - E.g. employee moral, company secrets
        - Monetary + psychological/emotional costs
- Always list assets with the most important first (impressions are formed early when reading).
- Verbs should be associated with asset nouns - i.e. is it the confidentiality of the data, or is it preventing it being changed, or losing it.
- Information to be gathered:
    - "How much money would you lose where this data center to go down for 24 hours?".
    - "How much will you lose if your company is disconnected to the internet for 3 hours?".

Examples of Assets

- Your life vs your wallet
- If someone keeps breaking your windows to get into your car, then your asset is your window, not your car, because that's what you have to pay to replace.
- The history of information
- Maybe losing something is more important than someone accessing it or stealing it
- Your reputation?

Bits of Security

- 10 bits of security = it takes 2^{10} operations to break the security.
- It is a measure of work to break some security

Entropy

- A measure of chaos
- English has low Entropy because it relies on a lot of patterns and ordering
- Because English has low Entropy, if you are decoding a message you will know when you have decoded the message. It is hard to decode a message into the wrong message.

Example

If we are given a key, of length 7, comprised of alphabetical letters:

- It would take **26^7 possible combinations** to brute force key.
- Most likely only 1 of the 26^7 key combinations would look like plaintext English
- 26^7 is the worst case amount of work it would take to solve the message.
- **Convert 26^7 into bits = $\log_2(26^7) = 32.9$**
- ^^ This is different from the original notes, but since there is a calculator in the exam this method is more accurate and works better
- Hence 26^7 = 33 bits of work (ceiling(32.9))
- This is crackable, as we need at least 128bits of work to make it too difficult for an attacker.

Another Example

- 2^60 operations required
- Need to make a lot of assumptions
    - How fast is the attacker's computer?
    - How many computers do they have?
- Assume they can do 2^{50} operations per second
- They need to do 2^{10} seconds worth of work in order to complete 2^60 operations which results in ~20 minutes of cracking. (more like 17mins)

Hash Properties

3 properties that a cryptographic hash function should have:

1. **Pre-image resistance**
2. **Second pre-image resistance**
3. **Collision resistance**

Pre-image resistance

- For essentially all pre-specified outputs, it is computationally infeasible to find any input that hashes to that output.
- I.e. given y, it is difficult to find an x such that h(x) = y.
- You can't reverse the hash / go backwards to find the input.

Second pre-image resistance

- It is computationally infeasible to find any second input which has the same output as that of a specified input
- I.e. given X, it is difficult to find a second pre-image Z != X such that h(X) = h(Z)
- Given an input X with output Y, you can't find a second input Z that produces the same hash output Y.

Collision Resistance

- It is computationally infeasible to find any two distinct inputs that hash to the same output
- i.e. such that h(X) = h(Z) where X != Z
- Not given anything, you can't find a two inputs that will collide in the same way.

With each of these properties, as long as an attacker has to use BRUTE FORCE to solve the problem, then your hash function has high-resistance. If the attacker knows of a way to do it faster than brute force, then your hash function has low resistance.

One-way function

- Attack against this is called pre-image attack

Collision free

- Attack against this is called Birthday attack
- · Random mapping is ideal
- Given a message, you hash it into a smaller message. It should just look like a random collection of things in the output.
- A small change in the input should ideally change on average half of the output / a diffuse effect
- Change in 1 bit should result in 50% chance of each hash bit changing.

Passwords salts

- You have a password and want to authenticate it but don't want to let the other party know your password, only the hash of your password. The hash of your PW will be stored rather than the true PW.

- However, the PW which belongs specifically to you can be worked out if the other party hashes every password that they have on file until it matches your one = **Dictionary Attack** on a pw / hash.
- You add extra “Salt” / data to your message / password before you hash it in. So the attacker does not have the advantage of **space/time trade-off** and can only attack 1 person but not everyone.
- If they want to attack everyone, they would need to create a whole new dictionary for each person, since everyone’s salt value is different.
- (because without the salt, if the attacker processes the hash of every password, they can store the result and do a parallel-attack by referring to what they’ve processed before)
- How many bits in a UNIX salt?
    - 4 bytes

Sessions

Session Timeouts also known as “Reaper Timeouts”

If a person leave an active session on, it can be attacked by unknown users who are looking to snoop or gain control of an account, by running programs they do not have access to. Session timeouts are designed to prevent unauthorized access and to control authorization levels. They could range from a few minutes to a few hours. An easy example would be a computer going to sleep to prevent another user from accessing it.
Message queue approach is a way of telling the user their session is about to expire. This is common in library systems.
System Values QINACTITV (inactivity time) system value determines the inactivity or timeout value. This is the amount of time (in minutes) that an interactive session can be inactive before the system performs an action.

Session Hijacking

Session Hijacking is like a Man in the middle attack, Session hijacking is where the hacker places a fake cookie pretending to be a real cookie. Cookies are automatically downloaded to a person's computer when they open a website so what the hacker can do is slip in a fake cookie and be a listener to your computer session.
There are 4 main methods used to hijack a session

Session Fixation - where the attacker sets a user's session id to one known to him, sending a user an email with a link that contains a particular session id. The attacker now only has to wait until the user logs in. Popular with fake emails

Session hijacking - here the attacker uses packet sniffing to read network traffic between two parties to steal the session cookie. Like network shark

Cross site scripting where the attacker tricks the user's computer into running code which is treated as trustworthy because it appears to belong to the server, allowing the attacker to obtain a copy of the cookie and to perform other operations.

Buffer Definition: Is where a program which is reading a buffer hits the boundaries and wants to read adjacent memory. When it over-reads buffer this is a violation and may cause programs to stall, crash or perform questionable acts. For example say the memory to be over-read is a piece of code that is design to do damage, and the program over reads which causes unexplainable behaviour. These are known as software vulnerabilities which may be exploited to attain information that is not authorized. A major reason to why buffer over-read, It is typically resulted from insufficient or lack of bound checking for buffer ready to work. So this comes down to coding practices. Poor stack frame and deallocation time of the stack frames is a leading cause of this buffer over-read problem.

Deep Packet Inspection

Deep packet inspection (DPI, also called complete packet inspection and information extraction or IX) is a form of computer network packet filtering that examines the data part (and possibly also the header) of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination, or, for the purpose of collecting statistical information that functions at the Application layer of the OSI (Open Systems Interconnection model). There are multiple headers for IP packets; network equipment only needs to use the first of these (the IP header) for normal operation, but use of the second header (such as TCP or UDP) is normally considered to be shallow packet inspection (usually called stateful packet inspection) despite this definition.

Remember Digital signature is very different to a digital certificate

Digital signatures

- are based on public key cryptography, also known as asymmetric encryption. Using a public key algorithm such as RSA, we can generate two keys that are mathematically linked: such as a private and public Key. One important note is that encrypting the hash instead of the entire message of the document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter and faster. And that hashing is faster than signing.
- Like all signature they can be defrauded.
- Digital signatures make it difficult for the signer to deny having signed anything (non-repudiation). Based on the assumption that the private key has not been compromised
- Digital signatures are also used to provide proof of authenticity, data integrity and nonrepudiation of communications.

Keys (Revisit)

Symmetric Key Mainly for encryption and decryption cannot be used for digital signatures integrity and nonrepudiation checks.

Asymmetric often creates a larger file. Symmetric square of the number of participants asymmetric scales up well. Asymetric has no problem with the key agreement. Symmetric requires you to agree on the key

Birthday Attack Example (revisit)

The birthday attack on digital signatures allows a third party to replace one digitally signed message with a different one without altering the signature. Consider the following situation between Alice, Bob, and Trudy. (As in most cryptography examples, messages go from Alice to Bob, while Trudy is an "Intruder" attempting to disrupt or intercept communication.)
Alice writes an e-mail to Bob with the following text: Dear Bob,

I would like to recommend Fred for the job of regional manager here at ConHuge Co. Ltd. Fred is an excellent employee...
etc, etc. Assume the message is at least a few paragraphs long. Now, Alice digitally signs the message (using PGP for example), then hands it to her secretary Trudy, and tells her to send it to Bob tomorrow. (Alternately, Trudy could intercept the message using more technical means, but we assume simply that Trudy simply has the message and can stop Bob from receiving it verbatim.) Let's say Trudy was also trying to get the regional manager job, and in any case does not want Bob to get it. She could write a message like this:
Dear Bob,

I think that Fred is a poor choice for regional manager at ConHuge Co. Ltd. His work record is terrible, he is frequently late...
etc, etc. The problem, of course, is that Trudy's message won't be digitally signed by Alice, because Trudy doesn't have access to Alice's private key, and it is computationally infeasible to get it from the signature. So how can Trudy forge the digital signature?
Very quickly, digital signatures work as follows. The message goes through what is called a One-Way Hash, such as MD5. This produces a hash value. Then, the hash value is encrypted using Alice's private key. Anyone can use Alice's public key to decrypt the signature and get the hash value. Then, they re-hash the message using the same algorithm. If the receiver's hash value matches the hash value in Alice's signature, then the message is assumed to be intact. If not, the message has been altered and should be discarded. Trudy can generate hash values on her messages, but she cannot generate the signature that is decryptable with Alice's public key. So what can Trudy do?
Well, Trudy writes a message like this:
Dear (Bob|Robert),

I (feel|think) that (Fred|Fred Smith) (is not|isn't) a (good|fair) choice for the (position|job) of regional manager. He is (frequently|often) late...
The words marked with (a|b) are alternatives. Either a or b is acceptable in producing a message with the same meaning. Now, Trudy writes a Perl script that generates all possible combinations of her message using all the alternative pairs. If there are n alternative words, then there are 2^n messages, which is quite a lot. The Perl script also verifies each of the 2^n messages against Alice's digital signature. It may take a few hours of computation, but given enough possible messages, eventually one will produce the same one-way hash, and thus will be valid with the same signature! (See EE's writeup for the mathematical reasons behind this.)
When Trudy has found a message that is valid, she can substitute it in Alice's message, and then put the digital signature on the end. When Bob receives the message, he will not be able to tell it's been altered.

Lessons from the birthday paradox

- **sqrt(n)** is roughly the number you need to have a 50% chance of a match with n items. sqrt(365) is about 20. This comes into play in cryptography for the birthday attack.
- Even though there are 2^{128} (1e38) GUIDs, we only have 2^{64} (1e19) to use up before a 50% chance of collision. And 50% is really, really high.
- You only need 13 people picking letters of the alphabet to have 95% chance of a match. Try it above (people = 13, items = 26).
- Exponential growth rapidly decreases the chance of picking unique items (aka it increases the chances of a match). Remember: exponents are non-intuitive and humans are selfish!

How to protect yourself against the birthday attack

One way to protect yourself against the Birthday Attack is to ensure the security of the transmission medium. For instance, you can send your messages through an SSH tunnel, and it will be much harder to intercept, (though not impossible). In some cases this is impossible. For instance, some e-mail servers won't support SSH, or if the mail is forwarded through multiple servers, you may not be able to guarantee the connections will always be secure.
You could also encrypt the message. If Bob had a an asymmetric key (as used in PGP), then Alice could have encrypted the message and signature and had it sent to Bob. In such a case, the only way Trudy could alter the message is if she had Bob's private key. This fails, however, if Bob does not use PGP or similar programs.

Birthday Paradox

The apparent paradox that, in a schoolroom of only 23 students, there is a 50 percent probability that at least two will have the same birthday. The "paradox" is that we have an even chance of success with just 23 of 365 possible days represented.
The "paradox" is resolved by noting that we have a 1/365 chance of success for each possible *pairing* of students, and there are 253 possible pairs or combinations of 23 things taken 2 at a time. (To count the number of pairs, we can choose any of the 23 students as part of the pair, then any of the 22 remaining students as the other part. But this counts each pair twice, so we have 23 * 22 / 2 = 253 different pairs.) Note that 253 / 365 = 0.693151.

Pre-Image Attack Recap

In cryptography, a **preimage attack** on cryptographic hash functions tries to find a message that has a specific hash value. A cryptographic hash function should resist attacks on its preimage.
In the context of attack, there are two types of preimage resistance:

- *preimage resistance*: for essentially all pre-specified outputs, it is computationally infeasible to find any input that hashes to that output, i.e., given y, it is difficult to find an x such that $h(x) = y$.
- *second-preimage resistance*: it is computationally infeasible to find any second input which has the same output as that of a specified input, i.e., given x, it is difficult to find a second preimage $x' \neq x$ such that $h(x) = h(x')$.

These can be compared with a collision resistance, in which it is computationally infeasible to find any two distinct inputs x, x' that hash to the same output, i.e., such that $h(x) = h(x')$. Collision resistance implies second-preimage resistance but does not guarantee preimage resistance.

By definition, an ideal hash function is such that the fastest way to compute a first or second preimage is through a brute force attack. For an n-bit hash, this attack has a time complexity 2^n, which is considered too high for a typical output size of n = 128 bits. If such complexity is the best that can be achieved by an adversary, then the hash function is considered preimage-resistant.
Faster preimage attacks can be found by crypt analysing certain hash functions, and are specific to that function. Some significant preimage attacks have already been discovered, but they are not yet practical. If a practical preimage attack is discovered, it would drastically affect many Internet protocols. In this case, "practical" means that it could be executed by an attacker with a reasonable amount of resources. For example, a pre imaging attack that costs trillions of dollars and takes decades to preimage one desired hash value or one message is not practical; one that costs a few thousand dollars and takes a few weeks might be very practical.
All currently known practical or almost-practical attacks on MD5 and SHA-1 are collision attacks. In general, a collision attack is easier to mount than a preimage attack, as it is not

restricted by any set value (any two values can be used to collide). The time complexity of the collision attack, in contrast, is $2^{n/2}$.

Looking at military weapons

- A simple and effective method to block IR is an ordinary ‘space blanket’ or thermal blanket of Mylar foil. The foil will block the IR heat signature behind it. A problem though, is that whatever it is that you are attempting to conceal, its heat will either build up inside to an unbearable degree or it will escape ‘somewhere’, which will then be visible to IR imagers. Concealment forthe most part will be temporary without elaborate mechanisms to disperse the heat signature.
- Drones and thermal vision have been held up to the common citizenry for years as the end-all-be-all of combat and surveillance technology.
- To hide from surveillance cameras use a mirror to create an illusion. Optical illusion is the best bet, what you see is different to what you are actually seeing

MODULE #06

One-Time Pads

The Process

- One time pads require XOR, and a key (which is randomly generated) that is the same length as the plaintext, which is then XOR'ed with the plaintext to form the ciphertext.
- The key, or the sequence of numbers comes from a one-time pad. This is the shared secret between the two people communicating. Each sequence of random numbers must only be used once. (hence the one)

Properties

- OTP creates a ciphertext that is unbreakable. You can't cryptanalyse the ciphertext, as any combination of numbers can result back to the original plaintext.
- The shared secret is extremely large. Both parties must have the one-time pad in order to communicate. The secret is as large as all possible messages you have may have to send.
- The key distribution problem is a big problem.
- Most encryption systems rely on turning a large thing into a small thing (the key). This means that we get collisions and patterns. Using a big secret to protect the message gives perfect protection.
- Claude Shannon showed that these were theoretically unbreakable.
    - They can be breakable however if they're not used the right way, an example being the russians in the war.
    - Once you've reused a key, because of the nature of XOR, you can then do statistical analysis, or a Crib Drag to get the messages back.

XOR

- *Uses XOR ⊕, which can be done with ~3-5 transistors, so it is an extremely fast operation. N.B. With XORing - if either of the input numbers is random, the output is random.*
- XOR works on bits.
    - $0 \oplus 0 = 0$
    - $0 \oplus 1 = 1$
    - $1 \oplus 0 = 1$
    - $1 \oplus 1 = 0$
- It's a reversible operation.

- It can also be thought of alphabetically, which is useful because it can work in the field. e.g. abcde ⊕ 12345 = (a+1)(b+2).... = bdfhj
    - KEY = key
    - PT = cat
    - CT = cat ⊕ key
    - c + k = 2 + 10 % 26 = 12 = m
    - CT = mfd
    - PT = mfd ⊕ key
    - 12 - 10 % 26 = 2 = c

More on XOR

- The widely-used assembly language mnemonic for the exclusive-OR function as a computer operation or opcode. Exclusive-OR is basically a Boolean logic function which is bit-level addition without carry. Normally, however, a computer will do a full word-width of exclusive-OR's, instead of operating just one bit at a time. Also called: "addition mod 2."

- The exclusive-OR function is the simple but strengthless additive combiner of a conventional stream cipher. Exclusive-OR is also used extensively in block ciphers and, indeed, throughout cryptography.

- The exclusive-OR function can be generalized beyond simple 2-value bit-elements to elements of arbitrary range in the Latin square combiner. The Ls combiner supports a huge number of unique, nonlinear, combining tables, and, thus, also supports combiner keying, which is simply not available with exclusive-OR

XOR Encryption

Usually, the simple stream cipher produced by XOR-combining *plaintext data* with a *keystream*. Commonly, the keystream is produced by a keyed random number generator. There is also a toy version which uses a short string of text or random values as the keystream. Both versions become insecure as soon as the keystream starts to repeat, so the toy version is insecure almost immediately.

In cryptanalysis we normally assume that the opponent has a substantial amount of both the original plaintext and the corresponding ciphertext (known plaintext). In that case, simply combining the plaintext and ciphertext in another XOR exposes the original keystream (a known plaintext attack). That means the keystream generator can be attacked directly, which implies that XOR has not protected the generator at all.

Confusion and Diffusion

Claude Shannon's two properties of a good cipher.

- Confusion – relationship between the **key** and the **ciphertext** is mysterious
    - Confusion destroys any relationship between the key and the ciphertext
    - Substitution ciphers.
- Diffusion – relationship between the **plaintext** and **ciphertext** is mysterious and highly variable
    - Diffusion spreads out and jumbles the relationship between the plaintext and the ciphertext.
    - Permutation Ciphers
    - Ideally we want the avalanche property; if one bit of the plaintext is changed, on average half of the ciphertext changes
- SP Networks are Substitution/Permutation Networks.

Symmetric and Asymmetric Encryption

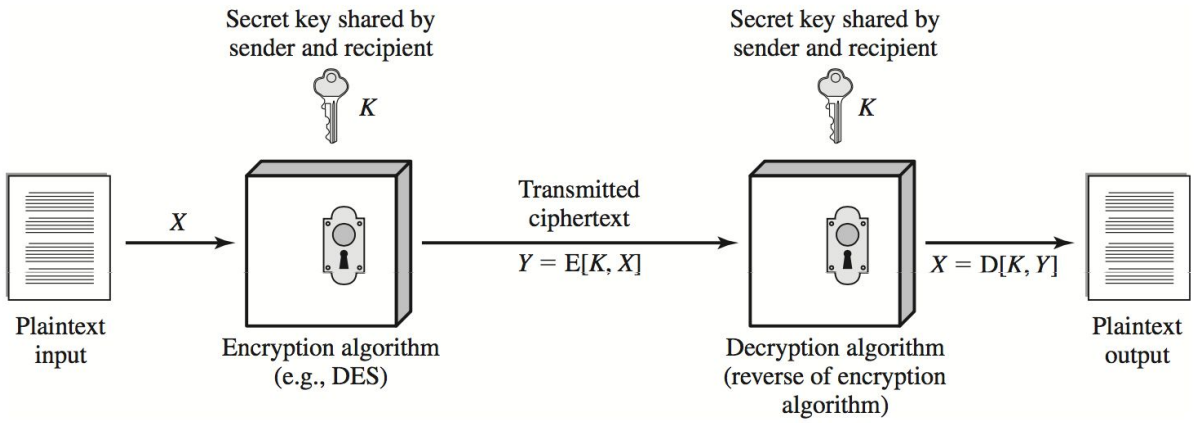
Symmetric Cryptography

- **Same key to encrypt and decrypt**
- One key per every pair, so for n people, ~n^2 keys.
- Key distribution is the challenge
- Simpler, faster, takes less resources
- Used by e.g. military - diff key for diff person, so even if one key is found not all conversations are compromised.
- Used in long sustained conversations (use asym first to establish key, then sysm from thereon) - SSL
- Used when you encrypt your own data - don't have to distribute the key.

Asymmetric Cryptography

- **different decryption key to the encryption key**
- Whilst solving key distribution, they are slow (involve complex maths), and introduce new problems.
- Slower
- Better than sym since you don't have to remember all keys - everyone has their own private and public keys.
- Better than sym since you don't need a secure channel to establish your private key. So if you need to have a secure connection in an unsecure medium. Just give your public key, and never have to give out your private key. SSL.

Symmetric Encryption



A symmetric encryption scheme has 5 ingredients:

1. Plaintext
    - The original message or data that is fed into the algorithm as input.
2. Encryption algorithm
    - Performs various substitutions and transformations on the plaintext.
3. Secret key
    - The secret key is also input to the encryption algorithm.
    - The exact substitutions and transformations performed by the algorithm depend on the key.
4. Ciphertext
    - The scrambled message produced as output.
    - It depends on the plaintext and the secret key.
    - For a given message, two different keys will produce two different ciphertexts.
5. Decryption algorithm
    - The encryption algorithm run in reverse.
    - It takes the ciphertext and the secret key and produces the original plaintext.

Requirements for secure use of symmetric encryption

1. Strong encryption algorithm
    - The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plain- text that produced each ciphertext.
2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.
    - If someone can discover the key and knows the algorithm, all communication using this key is readable.

Symmetric Encryption Attacking Approaches

1. Cryptanalysis
    - Rely on:
        - Nature of the algorithm
        - Some knowledge of the general characteristics of the plaintext
        - Some sample plaintext-ciphertext pairs
    - Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
    - If the attack succeeds in deducing the key, the effect is catastrophic:
        - All future and past messages encrypted with that key are compromised.
2. Brute-force attack
    - Try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
    - On average, half of all possible keys must be tried to achieve success.
        - If there are x different keys, on average an attacker would discover the actual key after x/2 tries.
    - It is important to note that there is more to a brute-force attack than simply running through all possible keys:
        - Unless known plaintext is provided, the analyst must be able to recognize plaintext as plaintext.
        - If the message is just plain text in English, then the result pops out easily, although the task of recognizing English would have to be automated.
        - If the text message has been compressed before encryption, then recognition is more difficult.
        - And if the message is some more general type of data, such as a numerical file, and this has been compressed, the problem becomes even more difficult to automate.
    - To supplement the brute-force approach it needs:
        - Some degree of knowledge about the expected plaintext
        - Some means of automatically distinguishing plaintext from garble (jumbled message)

Symmetric Block Encryption Algorithm

The most commonly used symmetric encryption algorithms are block ciphers. A block cipher processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block. The algorithm processes longer plaintext amounts as a series of fixed-size blocks.

The most important symmetric algorithms (and all of them are block ciphers) are:

- Data Encryption Standard (DES)
- triple DES
- Advanced Encryption Standard (AES)

Comparison of Three Popular Symmetric Encryption Algorithms

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

Average Time Required for Exhaustive Key Search

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/μs	Time Required at 10^{13} decryptions/μs
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	$2^{55}\,\mu s = 1.125$ years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	$2^{127}\,\mu s = 5.3 \times 10^{21}$ years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	$2^{167}\,\mu s = 5.8 \times 10^{33}$ years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	$2^{191}\,\mu s = 9.8 \times 10^{40}$ years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	$2^{255}\,\mu s = 1.8 \times 10^{60}$ years	1.8×10^{56} years

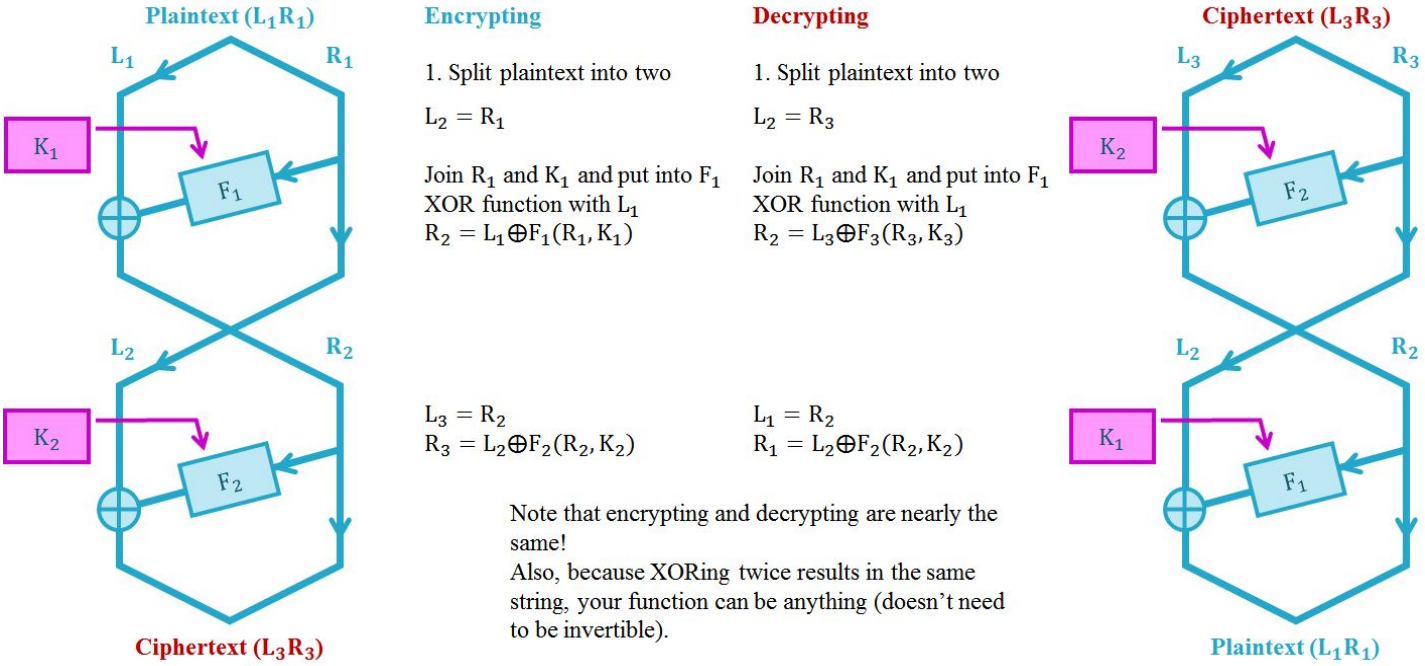
Note: a rate of one billion (10^9) key combinations per second is reasonable for today's multicore computers

Symmetric keys

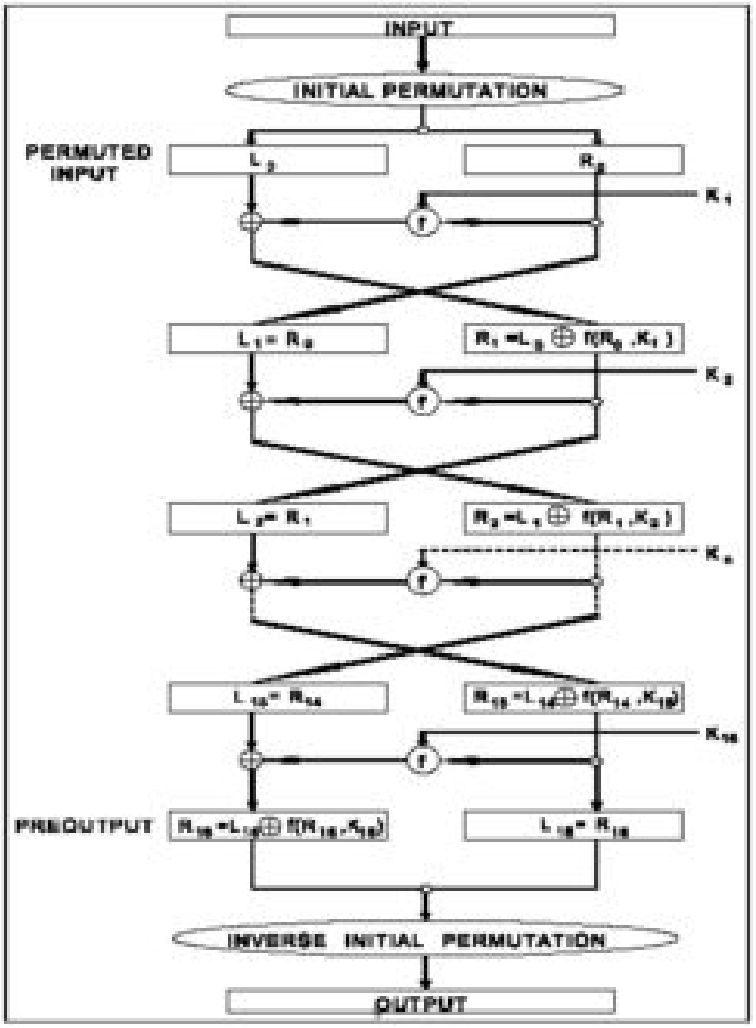
- Data Encryption Standard (DES) 55 bits of work – during WWI, encryption relied on no one knowing the secret, and adding junk in to be as confusing as possible
    - DES takes a plaintext block of 64 bits and a key of 56 bits, to produce a ciphertext block of 64 bits.
    - Donald Knuth wrote in semi-numeric algorithms on random number generation
    - a randomly generated number isn't as random – e.g. try plotting them in multiple dimension
    - a good number random number generator is to choose systematically the best way of detecting randomness is looking for all the possibilities that you know of
- Feistel network (DES)
    - 64 bit key (although only 56? are significant) gets converted into sub-keys → compare with concept of key extension
    - Subjective to differential analysis
    - The same key is used in encryption and decryption (symmetric cryptography) - very easy to implement in hardware
    - Doesn't have to be an invertible function (I.e. doesn't have to make the function go back)

DES

DES works by splitting a 64 bit plaintext in half, applying one half to an F function, which is just a series of substitutions through a lookup table, (that doesn't need to be invertible because of XOR) then XOR'ing that with the other half, and then swapping the two streams, then repeating this process 16 times.



1. Plain text comes in, then gets split in half (Say we start with 128bits)
2. One half (64 bits) and the first of the sub-keys is passed into a function (does not need to be invertible)
3. XOR above with the other half (other 64bit) of the message
4. Then do the same thing, but start with the other half.
5. Did this round 10 times.



Concerns on Strength of DES

1. Algorithm
2. Use of 56-bit key

AES (Rijndael) 192,

- Multiple rounds - every bit is invertible; the function used, is invertible
- Different number of rounds - what happens in each round is customised
    - Both a SE operation (substitution cipher) and P operation (permutation) occurs → gives confusion and diffusion
- Injects a new key into each round
- Most of the rounds can be backtracked
- Designed to be able to be coded within 120? bytes
- Key distribution problem: nc^2 → when the number of keys needed increases…. Squares
    - Relevant to symmetric, but not asymmetric (which are much slower)
- Perfect order security
    - Relevant to asymmetric, but not symmetric

- Another encryption: Blowfish
- Maths problems that are hold to solve e.g. factoring

Side channel attacks, DES used more energy when there was a 1 compared to when there was a 0, so could monitor the energy spikes to do attack on DES

Red-teaming (Fionnbarr talk)

- WPS in routers is insecure and can be brute forced because of its nature.
- Red is offensive team
- You have to be the enemy, and simulate that as real as possible
- Normal penetration testing, only have access to limited product/feature/page
    - But actual hacker, has access to the whole system, possibly to whole company, access to your nanny
- Red teaming, try find worst case scenario, attacking the whole company, work out what the attacker would actually want.
- Talk to company to work out what is valuable to the
- Phishing
    - Technical people get suss, but HR they might not get suss, they deal with a lot of files, just make a CV, throw in a bit of truth, then phish for info
- In the end, then talk to blue team and explain the vulnerabilities.
- Turkish oil company he worked out, he red-teamed for them and asked about their threats
    - Russia, Isis,
    - Worried about losing their CAD drawings, designs
- Social engineering

For the uninitiated, a ***biometric scanner*** reads the fingerprint of the user, instantly identifying them and allowing them to clock in and out. Whereas previous techniques involving badges and time cards relied just a little too heavily on trust (which can too easily be squandered) and the honor system (too easily taken advantage of), a biometric scanner can allow you to track the arrivals and departures of your employees with ease.
You might think that introducing a new technology into the workplace would cause a disruption, requiring you to train personnel to use and administrate it. With MinuteHound, that's not the case at all. There is virtually no learning curve, meaning no lost time and profits, and the software is plug-and-play. Furthermore, the technology that powers the MinuteHound biometric scanner is cloud-based, meaning management has access to employee time clock records from just about any computer, anywhere in the world.

This section is looking encryption standards for the government

Introduction

Cryptography, often called *encryption*, is the practice of creating and using a cryptosystem or cipher to prevent all but the intended recipient(s) from reading or using the information or application encrypted. A cryptosystem is a technique used to encode a message. The recipient can view the encrypted message only by decoding it with the correct algorithm and

keys. Cryptography is used primarily for communicating sensitive material across computer networks.
The process of encryption takes a clear-text document and applies a *key* and a *mathematical algorithm* to it, converting it into crypto-text. In crypto-text, the document is unreadable unless the reader possesses the key that can undo the encryption.
The Need for Data Encryption at DPW
In the course of normal business operations, staff at the Department of Public Welfare (DPW) is responsible for handling a variety of confidential data. IRS-derived financial data, HIPAA-related medical data, and personnel data are just a few examples of data that DPW must keep confidential. In addition, DPW is responsible for maintaining the integrity of confidential data.
Internal DPW policies, state laws, the policies of other partner agencies (for example, the Internal Revenue Service (IRS)), or federal laws may govern staff or business-partner access to confidential data.
These requirements may necessitate:

- Strong authentication of the entity requesting the protected data
- Limits on the data, and/or limits on the use of the data
- Encryption of the data for transmission
- Encryption of the data for storage
- Limits on the media on which the data is distributed
- Limits on the media on which the data resides

Please refer to *H-Net Data Classification Standards* for details on the various categories of data maintained by DPW and associated restrictions.

Purpose
The purpose of this document is to describe the cryptographic techniques standardized in the information technology (IT) field and deployed at DPW for secure communication within DPW and between DPW and its business partners.
This document outlines the acceptable levels of encryption for DPW and how they are applied to data transmissions, transactions on the Intranet, Internet, and other outside interactions (such as FTP), and data storage, particularly on portable devices.
Encryption Standards for DPW Data
DPW adheres to the following encryption standards for transmission and storage of confidential data. These are the minimum required standards. In cases where the federal, state, or other agency requirements are more or less stringent, the higher standard takes precedent.
Data Transmission
Secure Sockets Layer (SSL) or Virtual Private Network (VPN)
Use of either secure sockets layer (SSL) encryption (version 2 or greater) or a virtual private network (VPN) is the standard.
In the case of the VPN, determine the endpoints of the tunnel carefully, based on the security of the systems at each end. A client-workstation-to-server connection is best. VPN is necessary for file transfer protocol (FTP) exchanges that cannot employ SSL.
CheckPoint's SecuRemote and VPN-1 using shared secrets are currently the DPW standards for a VPN.

Pretty Good Privacy (PGP) encryption system is no longer a standard at DPW and is no longer supported. Though some transfers still use PGP, do not use it for new applications.

Encryption Type: Symmetric and Asymmetric

Though both symmetric and asymmetric encryptions are standard, you may want to use symmetric encryption for higher performance, though asymmetric provides better security. For the initial key exchange (distribution of the shared secret), use asymmetric encryption (Public Key Infrastructure (PKI)).

Key Length: Minimum 128-bit

Use minimum 128-bit keys for a symmetric cryptosystem.

Shared Secret Rotation: New Keys Every Five Minutes Minimum

Do not use fixed shared secrets. Generate and redistribute the shared secret keys at least once every five minutes in Windows 2000. This default (5 minutes in Windows 2000, and two minutes in Windows NT) has performance and security issues and can be adjusted in the following server Registry:

```
HKEY_LOCAL_MACHINE
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\ServerCacheTi
me
```

Do Not Use Wireless Devices

Currently, there is insufficient security for radio frequency wireless transmissions. Wired Equivalent Privacy (WEP), the encryption standard for wireless networks (Wireless LAN 802.11a & b), has been broken. Other issues such as parking lot sniffing remain a concern. Do not transmit sensitive data requiring access control and/or encryption (see *H-Net Data Classification Standards*) through wireless networks. Do not use wireless keyboards with such sensitive data.

Data Storage

Storage Device Security Depends on Data Security Requirements

Data that requires encryption for transfer also requires encryption while residing on an unsecured system. This includes storage on removable media such as but not restricted to floppy disks, CD’s, optical platters, zip disks, flash drives, storage/backup tapes, memory cards, etc., laptops and other portable devices (such as personal digital assistants (PDAs), cell phones, etc.) and may include desktops or servers.

A system is unsecured if the access control does not meet the minimum access control required by the data stored there. For example, data requiring a strong password could not be stored on a Windows 95 or Windows 98 operating system because strong password protection is not available on those operating systems. Another example is restricted data stored on a workstation shared by more than one user, or where there is the potential for other users to legitimately access the workstation. When those users log on to the system with a strong password, any user has access to the data stored there. Please refer to the *H-Net Data Classification Standards*.

Protect the BIOS and local user accounts of portable devices with a strong password to make them secure.

Encryption: Minimum 128-bit symmetric encryption

Use at least 128-bit encryption for symmetric encryption. You can use the Encrypting File System (EFS – based on the Expanded Data Encryption Standard (DESX) cryptosystem) native to Windows 2000 (or, for business partners outside of the Commonwealth, Windows

XP Professional) where available, or use a third party encryption program. At minimum, protect all private keys stored on the system with a password.
Before implementing any of the many third-party encryption programs available, DPW staff must review and approve its use for the given situation.
Lifetime: Store Data on PCs and PDAs Only When Using Data
When using workstations and portable devices (including laptops), store the data for the minimal time that it is required for its use. In the case of regular system backups (whether performed locally or over the network), encrypt the data before the backup, or do not backup the data.
Deletion: Use File-Wiping to Delete Data After it has Expired
Delete data as soon as it has expired, using a file-wiping program. Simply deleting a file does not remove the image of the data from the hard drive and is insufficient for secure removal of data from a system. Use a program such as Eraser, or, where available, use the file-wiping application native to the operating system, which, at a minimum, meets the United States Department of Defense recommendation 5220-22.M (January, 1995). This involves at least three passes of overwriting the entire “deleted” file with random bits and their complements.
PDAs: Do Not Put Sensitive Data on PDAs
An adequate encryption system (as described above) is not available for PDAs (Palm Pilots, iPAQs, Blackberry, and so forth). These devices are very portable and subject to loss and theft. Without adequate encryption of data to protect the data in the event the device is lost, do not store sensitive data (see *H-Net Data Classification Standards*) on a PDA. The Commonwealth is developing standards for the use of PDAs.

In the Government, digital services projects too often fail to meet user expectations or contain unused or unusable features. Several factors contribute to these outcomes, including the use of outdated development practices and, in some cases, overly narrow interpretations of what is allowed by acquisition regulations. OMB is developing tools to significantly upgrade the ability of Government digital services to deliver better results to our citizens and improve the way we capitalize on information technology (IT[1]) to better serve the American people.

One tool is the *Digital Services Playbook*, which identifies a series of “plays” drawn from proven private sector best practices to help agencies successfully deliver digital services. Another tool is the *TechFAR*, which highlights flexibilities[2] in the Federal Acquisition Regulation (FAR[3]) that can help agencies implement “plays” in the Playbook that would be accomplished with acquisition support.

The vision for the TechFAR is that it will be expanded in future iterations to address many areas of IT. This edition of the TechFAR is aligned with the Digital Services Playbook’s guidance to use contractors to support an iterative development process. In particular, it emphasizes Agile software development,[4] a technique for doing modular contracting and a proven commercial methodology that is characterized by incremental and iterative processes where releases are produced in close collaboration with the customer. This process improves investment manageability, lowers risk of project failure, shortens the time to realize value, and allows agencies to better adapt to changing needs. Agile software development

is geared towards projects where significant design and development are needed, such as digital services (e.g., healthcare.gov or recreation.gov) as well as internal digital services and business systems. It is not designed to be used for commodity IT purchases, especially where commercially available off-the-shelf items can be used as-is at a lower cost and lower risk to the Government.

In every agency, there are multiple stakeholders who share in the responsibility for achieving successful results from their IT investments and who form the acquisition team, including program officials, IT officials, acquisition officials, and agency legal counsel. Agencies need to ensure adequate resources are dedicated to these stakeholders involved in Agile software development efforts. The TechFAR is designed to facilitate a common understanding among these stakeholders of the best ways to use acquisition authorities in making these investments to level set expectations and maximize the likelihood for success. The TechFAR consists of a handbook, which discusses relevant FAR authorities and includes practice tips, sample language, and a compilation of FAR provisions that are relevant to Agile software development.

This handbook is not intended to usurp existing laws, regulations, or Agency policy. It calls out specific sections of the FAR as examples, but the TechFAR should not be read too narrowly to only apply to the sections specifically mentioned. All Federal agency stakeholders are encouraged to use this guidance. It is a living document; users are urged to provide feedback, share experiences, and offer additional strategies, practice tips, policies, or contract language that may be used to assure that IT acquisitions achieve their desired results. This feedback will be used to inform where additional guidance or reference materials may be appropriate.

The President's Management Agenda lays the foundation for creating a 21st century Government that delivers better results to our citizens and improves the way we deliver digital services to better serve the American people. This foundation includes an efficient and effective acquisition system that maximizes the value of every taxpayer dollar invested in technology.

The FAR and each agency's supplement to the FAR, set forth Government-wide overarching Federal procurement principles, policies, processes and procedures on procuring goods and services, including IT and digital services. The FAR provides contracting officials with considerable flexibility to conduct their acquisitions in smart, innovative ways that take advantage of proven commercial strategies. The TechFAR Handbook focuses on provisions of the FAR that are most relevant to digital services acquisitions and explains how agencies can align their applications of FAR authorities with contemporary development[1] approaches that improve investment manageability and budgetary feasibility, reduce risk, and shorten time to value. It is designed to support effective risk management and break down common myths that inhibit the modernization of Government's approaches to digital service development.

Within the realm of IT acquisition, this handbook concentrates primarily on software development procurements (excluding non developmental and commercially available

off-the-shelf items) and, in particular, the use of Agile principles. Software represents a significant component of IT contract[2] spending and plays a role in the success of most, if not all, Federal programs. The handbook assumes familiarity with OMB's Digital Services Playbook, which discusses strategies and best practices for agencies building digital services, and specifies Agile, iterative development as a critical component for success.

For each stage of the acquisition lifecycle, this document highlights key regulatory provisions and explains how Agile approaches can be effectively and successfully implemented consistent with core values of public procurement, including impartiality, accountability for results, and providing the best value to the taxpayer. It does not teach Agile software development, but includes practice tips and sample language from agencies that have successfully used these tools to support mission needs.

Analysis of FingerPrints

Several fingerprint scanners have been recently introduced in the biometric market, so that it is quite difficult for inexpert users to understand the technological differences and the features which determine the scanner quality and performance.
The most widely used scanner technologies are: optical and capacitive

Capacitive scanners are characterized by a small sensing area, not robust with respect to mechanical damage and electrostatic charges, requiring very high maintenance costs if the sensing element wears out. They need more frequent cleaning, to remove from the sensor surface deposits of grease or dirt left from the fingers, which highly deteriorate the quality of the acquired images. They are more suitable for use with cell phones and personal digital assistants.

Optical scanners use USB or parallel port connections and can stand alone or be built into other peripherals. The optics-based system is physically stronger than semiconductor-based systems in terms of impact-resistance, scratch-resistance, weather-durability and corrosion-resistance. Physical strength is a KEY factor for versatile outdoor usage. They perform better and are more durable than silicon-chip devices.
Over long periods of time, the optical-based scanners are more durable, require less maintenance, are more accurate with their failure rates, i.e., FAR (False acceptance rate) and FRR (False rejection rate) at the bare minimum.
FX2000 is an optical scanner. It's features are given below, detailing why it is most superior in quality as well as in performance:

1. RESOLUTION : The technical parameter to which people generally attribute the main importance is the resolution, that is the number of pixel per inch (dpi) characterizing the acquired images. Intuitively, the resolution indicates the magnification or zoom factor of the scanner. A 500 dpi resolution is required by FBI-compliant systems. 250-300 dpi is probably the minimum resolution which allows minutiae to be detected in the fingerprint pattern.

The figure below compares the same fingerprint portion as acquired at 500 dpi and at about 350 dpi. FX 2000 is a scanner that operates at a resolution of 569 dpi, even greater than that required by FBI.
Bits of security: Typically, images captured this way are 512×512 pixels (the dimensions used by the FBI), and the standard image is 2.5cm (1 inch) square, 500 dots per inch, and 256 shades of gray.
512*512 = 262144 (2^18)
256 shades of grey per pixel = 2^8
500DPI => 500 pixels per inch
Therefore: 2^18*2^8=2^26 … 26 bits of security. On average 13 bits of work.

MODULE #07

ACSC survey

ACSC (Australian Cyber Security Centre) survey reveals interesting statistics and facts related to cyber security in the last two years:

- 86% of companies have experienced an attempt at a cyber attack
- 58% were successful attacks and compromised the confidentiality, integrity or availability of their network data or systems
- Most of these have attacks have been from malware and social engineering fraud sources
- Social engineering attacks are increasing substantially over malware and attempted more often
- Example: Real estate transactions only need access to ONE critical email about which accounts to pay to to launch a successful attack

Organisations are controlled by a small group of people at the top of the hierarchy, hence hackers may target these people in order to get the most power.

CIOs set up the infrastructure, what security people or employees find out are therefore very likely criticism to them. Hence reporting to the CIO is not such a good idea. Reporting to the risk people or the CFO is a better idea.

Knowledge is power

- If you know any security-related vulnerabilities before everyone else then you have advantage
- This is seen in the case of the Borussia Dortmund football team bombing recently which may have been a financial attack on the share price as it gives the attacker advance knowledge of a share price drop which gives them financial advantage
- You can make great impact by having advanced knowledge on something. Another example is 'Insider trading' where someone knows some insider information (e.g. a merger that's going to happen because they're an employee of the company) and acts on it for private interest (e.g. buy shares before the price goes up because of the merger)

Side channel attacks

- Side channel attacks are where you take advantage of information that has been unintentionally leaked due to the implementation of a system.
- Side channel attacks are a form of reverse engineering.

Examples

- Someone can gain data by looking at the worn keys of a security keypad
    - Worn security keypads, worn-down buttons giving hints to what the passcode is. The worn pads on this keypad is an example of information leakage.

- Someone can analyse the energy input/output of a system and get the key to an encryption without the need to analyse the cipher text.
    - For example, electrical circuits emit sounds which allows an attacker to deduce how the circuit works and what data it is processing without accessing the circuitry itself
- Someone may leak information while transferring certain information, for example, If you sent someone a screenshot of your conversation, someone could tell who you've talking to by looking at the background of the screenshot, where they don't expect you to look.

General Classes of Attack

- **Cache attack** — attacks based on attacker's ability to monitor cache accesses made by the victim in a shared physical system as in virtualized environment or a type of cloud service.

- **Timing attack** — attacks based on measuring how much time various computations (such as, say, comparing an attacker's given password with the victim's unknown one) take to perform.
- **Power-monitoring attack** — attacks that make use of varying power consumption by the hardware during computation.
- **Electromagnetic attack** — attacks based on leaked electromagnetic radiation, which can directly provide plaintexts and other information. Such measurements can be used to infer cryptographic keys using techniques equivalent to those in power analysis or can be used in non-cryptographic attacks, e.g. TEMPEST (aka van Eck phreaking or radiation monitoring) attacks.
- **Acoustic cryptanalysis** — attacks that exploit sound produced during a computation (rather like power analysis).
- **Differential fault analysis** — in which secrets are discovered by introducing faults in a computation.
- **Data remanence** — in which sensitive data are read after supposedly having been deleted.
- **Software-initiated fault attacks** — Currently a rare class of side-channels, Row hammer is an example in which off-limits memory can be changed by accessing adjacent memory too often (causing state retention loss).
- **Optical** — in which secrets and sensitive data can be read by visual recording using a high resolution camera, or other devices that have such capabilities (see examples below).

Key lesson: You would be surprised by how many things leak information around you! The way we interact with objects or how the objects work may give away information without the user being aware of it, examples include timing attack, power attack, sound attack. You could prove algebra but not security. The way we build up security is through formalising properties and using algebra (or other methods) to prove these properties. So information we never thought of could easily become vulnerability in the system.

"Top men"

- The idea that we can trust "experts" who have designed a perfect system where nothing will go wrong

You can't rely on 'top men' for security. The real way to mitigate risk is the process - (e.g. review, scrutiny, testing, rigorous analysis, attempts to prove, lots of eyes on it) that matters.

Examples

- In court, prosecutions often rely on information provided by experts (i.e. the judge) but the judge isn't always right as evidenced by a study into which demonstrated guilty sentences are more likely before a judge has lunch, especially just before than after.
- DNA testing is often validated by "DNA experts" where the results turned out to be incorrect

Security lessons

- Everything needs openness and scrutiny- there is no justification for "Not needing it in this particular case"
- People that say "Trust us" should never be trusted - they are clearly not security engineers and don't sufficiently value or understand security and risk

The process for a security assessment:

1. Assets
2. Threats
3. Threat model
4. Mitigation

Building up a Threat Model

What sort of attacker are you defending against?

- What is a threat model: Systematic approach to list out possible sources of attacks.
- Consider the scope of the problem: What are the consequences of acting? What are the consequences of not acting?
- Consider the motives of possible adversaries
    - And what they gain from the asset that is being protected.
- **Systematic Analysis** - needs to be systematic, otherwise you will overlook aspects.
    - Prioritising sources of attack: a categorised and ordered list.
    - Threat Tree
        - Assets are nodes, threats are edges.
        - Causes of threats are sub-edges.
        - Used to enumerate the threat.
        - Need to consider all types of threats (boring sources, dramatic ones too). Don’t just think of the obvious sources.

Threat Trees

- Start with the asset

- Look at attacks/threats
- Start with broad categories, and slowly become more specific.

Dealing with Threats

- You always come up with better solutions when you think about things in **advance**, rather than under the pressure/adrenaline of the moment. These solutions thought in advance are developed with analytical, wiser considerations.
- Let ideas flourish for a little while, before criticising and killing ideas. You might kill an idea too early, but you have to be critical later.
- Ask questions for every way of dealing with threats. If they can't be answered, realise that herein there is a weakness in the system.
- When you defend, you have to defend appropriately given the potential attacks.

Magic tricks are like social engineering attacks

- Magic tricks are more about understanding human weakness and using it against them rather than technical abilities
- The important thing is to make sure that people are never concentrating on the things they should be concentrating on just like a social engineering attack
- Example trick - magic handkerchief, coin and wine glass procurement out of thin air trick - this exploits human susceptibility to suggestion which diverts their attention to the wrong thing
- Another trick - the famous three card monte trick. Three cards, one queen. Find the queen. This exploits the greedy human weakness.
- **Misdirection** is the ultimate attack on human weakness. It is when we are forced to pay attention to the wrong thing.

MODULE #08

Review - Bits of security Walkthrough

Passwords

Guess the 6 character password of someone - where the password is all in lowercase letters, except possibly **the first letter is uppercase (the first letter can be either uppercase or lowercase)**.

[A-Za-z][a-z][a-z][a-z][a-z][a-z]

52 x 26 x 26 x 26 x 26 x 26 ~ 617 millions

1 million ~ 2^20, 617 ~ 512 = 2^9 so worst case is 20+9 = 29 bits of work

average case will be 28 bits of work instead (since $2^{29}/2 = 2^{28}$)

Note: For exact number, consider using log base 2 instead.

Which case should we consider - worst case or average case?

Depends on which POV you are considering:

- Defender POV = average case
- Attacker POV = worst case

Identity and Authentication

Authentication is the trickiest part of security properties (CIA).

Computer mind model

- A computer is a like someone sitting in a dark room with a screen displaying input which is their only interaction with the outside world.
- If the screen displays the message “It's mum, push unlock button please", There is no way to know if that message was really sent by mum or not.
- The shared secret is the main key to distinguishing between the authorized person and the attacker. However, this shared secret is leaked by using it and the attacker can eavesdrop and replay the false authentication signal after notice enough pattern which means it does not remain secret forever.

How do we convince the computer that our authentication is correct?

Make the shared secret has randomness to make replay attack more difficult.
The challenge response can protect replay attack by asking the other side from given response e.g.

- Someone calls you to ask for your credit card no. and you said you will only give it when you have their phone number to call back later
- Multi factors authentication
    - OTP SMS
    - 2 Factor Authentication app

Recommended Book:

- Command and Control
    - President and General want to be the one who controls the nuclear launch
    - President get control in the end

Factors of Authentication

1. **Something you know** (Knowledge Based Authentication)
    - A secret that you know but nobody else does
    - Examples
        - Passwords
        - Shared Secrets
        - Challenge/Response (Uses the shared secret in some way)
    - Caveats
        - It can be used by someone else
        - You can forget
        - It is discoverable either by brute force or sniffing
    - Protection
        - Salting
        - Making protocol more secure from sniffing/eavesdropping
2. **Something you have** (A Physical proof of ID)
    - Any item that shows your authentication
    - Example
        - Driver license
        - Passport
        - Key card
        - Phone verification message
    - Caveats
        - It's forgeable
            - Fake ID / passport
        - It's must be with you when use
3. **Something you are**
    - Something that a person is

    - Example
        - Biometrics
            - Fingerprints
            - Iris (eye scanning)
            - Photo ID
            - How you walk
            - Dental Records
    - Caveats
        - It's unchangeable
            - If someone gets a copy of your fingerprints, you cannot change your fingerprint to be a new one
4. Vouching/Third party Verification

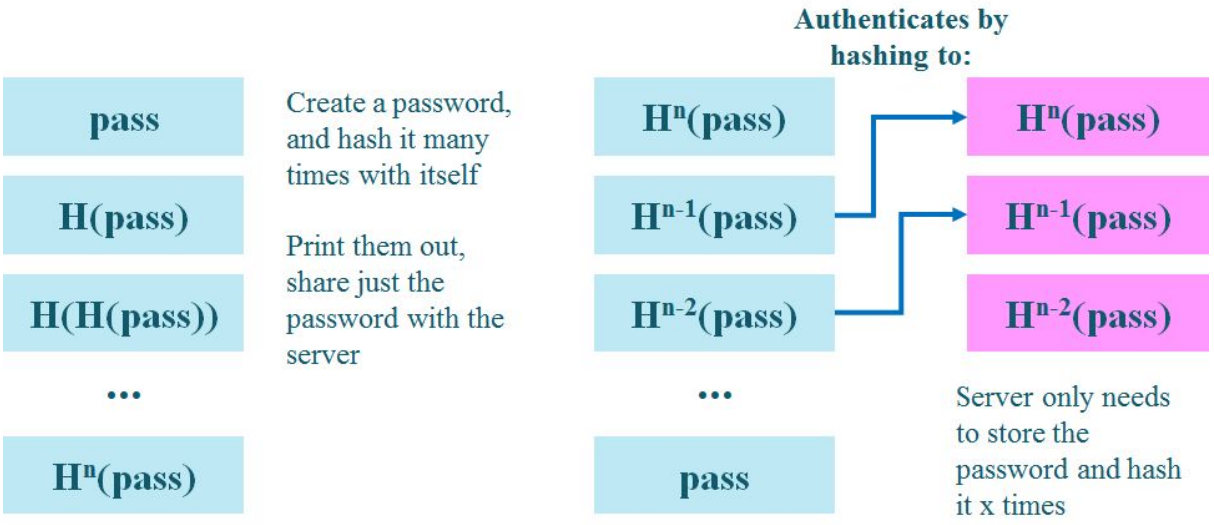
Multi-Factor Authentication

Knowing multiple things in order to get authenticated e.g. know account password and SMS verification code to sign in to an account.

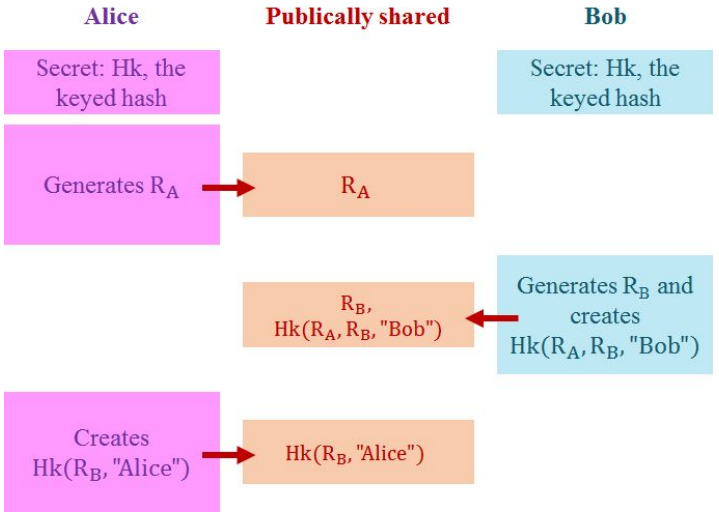
Simple Authentication Protocols

Challenge response

- Send secret, host compares
- Send secret, host store hash
- salt
- Send message encrypted with secret
- SKEY - f(f(f(f(r))))
    1. You start with an initial secret, r
    2. The system stores in the final value after applying f, (the hash) multiple times to that secret
    3. You then send the system the second last value, and the system hashes that and checks that it’s the same as the last value.
    4. The system then replaces the last value with the second last value.



- SKID
- Hk is keyed MAC both know k e.g. Hk(n) = 57
    1. A chooses + sends Ra (Alice's random number) to B
        - A ---------- Ra ----------> B
    2. B chooses Rb (Bob's random number), sends Rb, Hk(Ra ,Rb ,Bob's Name)
        - A <---- Rb, Hk(Ra, Rb, "Bob") ---- B
        - Need Ra for replay attack prevention
        - Need Rb to prevent man in the middle attack (MITM)
        - Need bob's name to stop a symmetry attack
    3. A sends H(Rb, Alice's Name)
        - A --------- Hk(Rb, "Alice") --------> B
        - Now each party knows their shared secrets



- Public Key Exchange
- Interlock Protocol (RSA)

Authentication vs Authorisation

Who am I vs What can I do

- Authentication = Who is this person?
- Authorisation = Does this person has permission to do something?
- *Authorisation depends on authentication.*
- Example: Airport
    - Authentication = Check-in + printing boarding pass
    - Authorisation = Check if the passenger goes to the right flight

TOCTTOU (Time of check to time of use) error

- Authentication vs Authorisation is a problem when they happen at different times, this leads to TOCTTOU errors.

In Unix, the following C code, when used in a setuid program, has a TOCTTOU bug:

```
if (access("file", W_OK) != 0) {
   exit(1);
}

fd = open("file", O_WRONLY);
write(fd, buffer, sizeof(buffer));
```

Here, access is intended to check whether the real user who executed the setuid program would normally be allowed to write the file (i.e., access checks the real userid rather than effective userid).

This race condition is vulnerable to an attack:

Victim	Attacker

if (access("file", W_OK) != 0)
{
  exit(1);
}
 	
fd = open("file", O_WRONLY);
// Actually writing over
/etc/passwd
write(fd, buffer,
sizeof(buffer));
	//
	//
	// After the access check
	symlink("/etc/passwd", "file");
	// Before the open, "file" points to the password database
	//
	//

- In this example, an attacker can exploit the race condition between the access and open to trick the setuid victim into overwriting an entry in the system password database.
- TOCTTOU races can be used for privilege escalation, to get administrative access to a machine.
- Although this sequence of events requires precise timing, it is possible for an attacker to arrange such conditions without too much difficulty.

- The implication is that applications cannot assume the state managed by the operating system (in this case the file system namespace) will not change between system calls.

Homework

- Try lifting up fingerprints/fool iPhone Touch ID
- Estimate bits in biometrics e.g. fingerprint, eye scan, facial recognition (it is surprisingly low)
    - How many faces the software able to recognize?
- How to prevent MITM?
- Find counterfeit coin/note/stamp/ID card/ticket

Identity Theft

- Once someone has stolen your identity, they retain it because your identity doesn't change.

Highlights for 2016:

- Costs to victims (direct+indirect) $2.2Billion
- 8.5% of respondents experienced some form of misuse of their personal information in the previous 12 months, with 4.9% of all respondents incurring out-of-pocket losses as a result of this misuse.
- DL - $500, Passport $5k
- IDCARE found that the misuse of identity on average occurs 72 hours after the initial compromise, with the majority of these incidents (87%) first detected by the victim. In the majority of identity theft incidences, the credential information is misused while only 16% reporting it to police.
- Identity Theft is the misuse of their personal information to do other thing on victim's behalf without their consent.

What data do they want?

- Your personal information
- Your ID
    - Driver license is the most popular target
    - Birth certificate
    - Credit Card
    - Passport

What is done with the data

- Take out loans - you can be liable
- Social security
- Claiming tax refunds on your behalf
- Commit crimes
    - E.g. speeding fines
- Purchase items that require identification
    - E.g. phones
- Credit cards
- Buying phone

People’s Response

- Embarrased
- Unaware they are a victim of a crime
- Don’t think reporting it will do anything
- Have had no net economic loss
- Confused about who to report it to

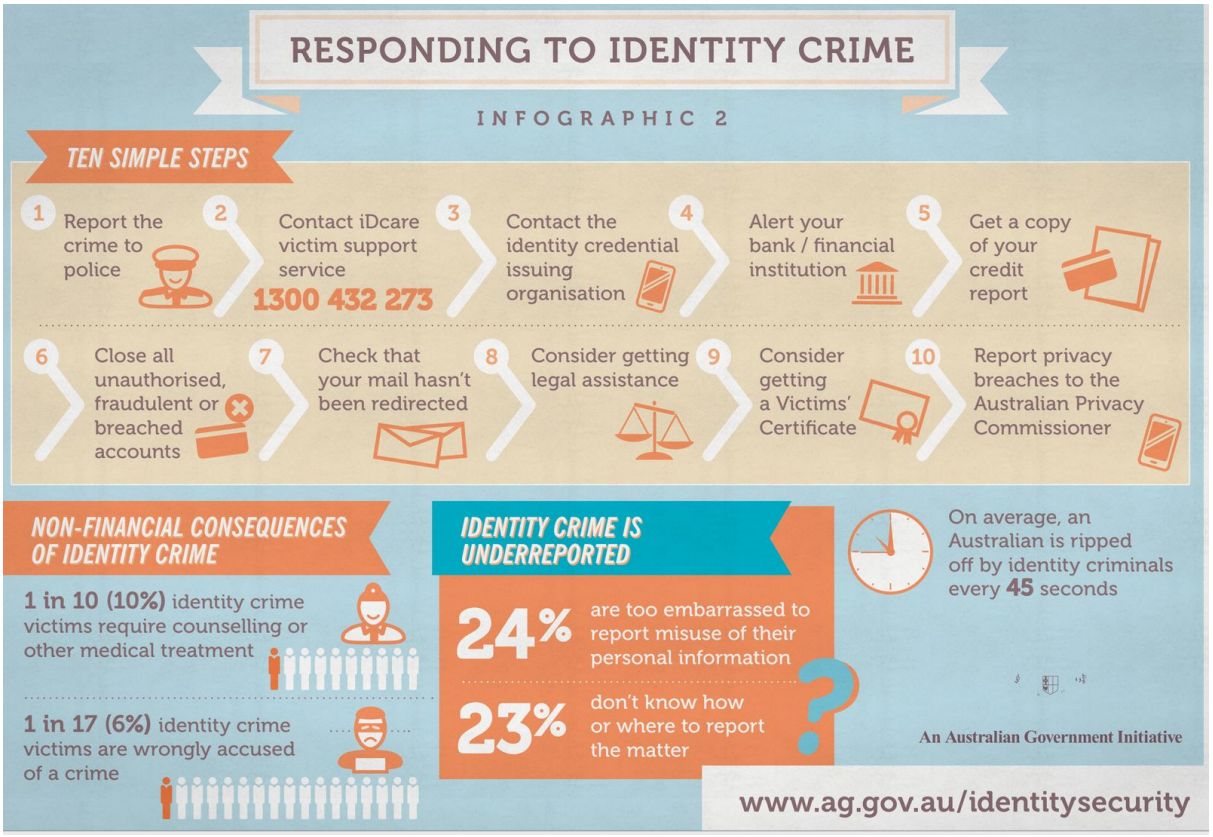
How to respond

1. Let bank and financial institution know
2. Call police
3. Call IDCare
4. Contact the identity credential issuing organisation
5. Get copy of your credit report
6. Close all breached account
7. Check mail hasn't been redirected
8. Get legal assistance
9. Consider getting victims' certificate
10. Report privacy breaches to Australian Privacy Commissioner

Impact on Identity Theft

- Unknown bank account that was opened under your name to do some mischievous transaction
- Your credit or loan was being rejected with strange reason that you didn’t do

What to do if you are a victim to Identity Theft?



If you are totally blank on what to do, contacting www.idcare.org (non-profit organization) is a good idea since they can help assessing risk you might have and provide action list on what to do next. For example:

- advise police, contact banks, credit report, request credit ban, check for mail redirections, close bogus accounts,
- change passwords from clean machines at clean location,
- be prepared for follow on scams.
- consider getting a **Commonwealth Victims' Certificate** from a magistrate
- report it at
    - ACORN http://www.acorn.gov.au/ and to the
    - ACCC online scam reporting site “Scamwatch” https://www.scamwatch.gov.au/report-a-scam
    - If the attacker was outside of Australia e.g. Russia, consider reporting to Europol instead https://www.europol.europa.eu/report-a-crime/report-cybercrime-online

Prevention

- check your credit rating and history every year
    - idcare http://www.idcare.org/credit-reporting/ provide list of Australian credit agency that you can use to request ban or request your credit rating report

Agency	Request Ban	Order Report
Experian	http://www.experian.com.au/credit-services/credit-reports/place-a-ban.html	http://www.experian.com.au/credit-services/credit-reports/order-credit-report.html
Dun & Bradstreet (D&B)	https://www.checkyourcredit.com.au/Resources/Forms/BanApplicationForm.pdf	https://www.checkyourcredit.com.au/MyAccount/Order/StandardService
Equifax (formerly Veda)	banrequestAu@equifax.com	https://forms.mycreditfile.com.au/Apply/Index?form=FreeCreditFile&_ga=1.15153846.1072713756.1426549134

    - e.g. see https://www.moneysmart.gov.au/
- Document Verification Service
- National Facial Biometric Matching Capability = FVS (AG)

Further read:

- Identity crime and misuse in Australia 2016
- Identity crime and misuse in Australia 2013-2014

Privacy

The main problem is how to balance between privacy and security

Stories

The High Street Abductions

- English policemen can find the missing girl on time before she was abducted by human trafficking gang because there are CCTV camera all over the city.
- In the other point of view, people in the city are being monitored.

MODULE #09

Trust and the Problem of Key Distribution

- Data and control are often intertwined, it's very hard to separate the two.
- For example, a self driving car that enforces speed limits. That is combining data and control.
- By changing the data we change the control the system, allowing attacker to attack the data to manipulate control.
- As soon as you have a system that makes control decisions based on data, you have an attackable system.

Phishing

- Authentication is a problem we haven't solved well yet in security
    - In past times, impersonation was hard, but now it's a lot easier, often with no physical risk to the imposter
- Clicking a link in an email is just playing Russian roulette
- You can spoof the from address of an email easily (you can check the outgoing server)
- CommBank doesn't send you emails, it notifies you that there is an email in your inbox
    - Using an unsafe channel as a trigger for you to check the trusted channel (logging in to check your inbox)

If you're in a dark room, how do you know that the stream of 1's and 0's is coming from who you think it is?

- Shared secrets are a partial solution - but secrets leak and can be replayed.
    - We can't know that no one else knows the shared secret, until it's too late
    - Nonce's help prevent replays.
    - Something you know, something you have, something you are - factors that can be used in authentication.
- The challenge is we need a way of distributing shared secrets, and spoilers, none of them are a much good.
- One problem is that you think you're authenticating one thing but it's actually another.
- Shared secrets are only useful for authenticating someone you've talked to before. But what if you want to communicate with someone you've never talked to before?

Non-repudiation

When authenticating yourself, there is usually a shared secret. This means that neither you or the authentication system can prove the authentication without revealing the secret. Hence, there can be repudiation (deny the authentication).

How can we get non-repudiation?
Use asymmetric keys:

- Can use the same key to prove authentication with different systems
- Digital signatures

Horton Principle

- Horton Hatches the Egg. ("I meant what I said, and I said what I meant. An elephant's faithful, one hundred per cent!")
- Horton Principle (a design principle for cryptographic systems): Authenticate what is being meant, not what is being said.
    - Often this is a disparity between what people want to authenticate/validate/check, and what we actually do, and in this divide there is vulnerability to being fooled by someone

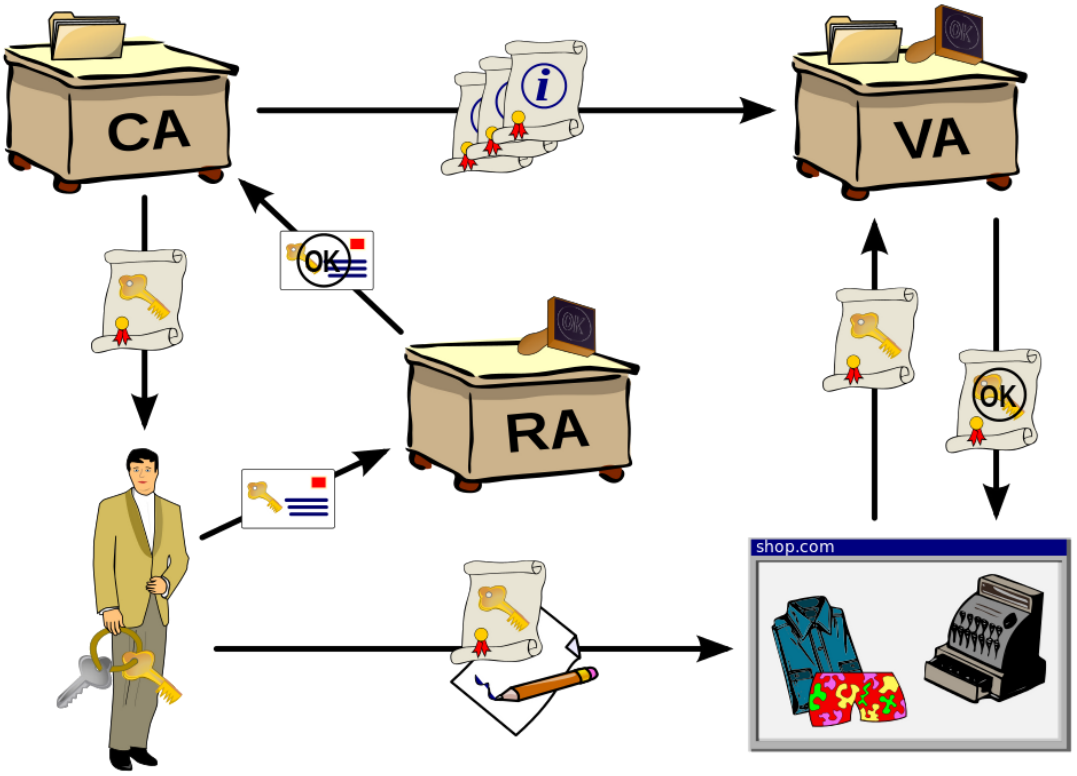
Two Approaches:

1. Centralised authority based Command and Control - eg. PKI
    - most obvious weakness: single point of failure
2. Decentralised peer based web of trust - eg. PGP, Blockchain
    - I trust that x would have already realised that the person I am talking to isn't the person I am talking to
    - How do I know that Richard is Richard? I know because the a lot of the tutors know and I trust the Tutors.

Public Key Infrastructure (PKI):

- Based on standard called X.509
- Generally used on the internet (SSL certificates)
- What's the problem with asking for the person's public key, and then using it to encrypt?
    1. Man in the Middle. Eve could intercept messages from Bob and send their own public key on to Alice, and pretend to be each person.
- Solution: a "bank" of public keys - SSL certificates
    1. Certificate Authorities (CA)
    2. Web browsers come preloaded with the public keys of the certificate authorities.
    3. Bob sends Alice a certificate that has been signed using the CA's private key. Using the CA's public key, you can figure out that the certificate is valid.
- A CA certifies the identity of an individual through extensive vetting and if satisfied provides a signed certificate confirming the identity, encrypted with a private key held

by the CA. So people communicating with this individual can use the CA's public key to decrypt it and verify the certificate.



Certificate authority

- You trust the CA, you use the CA to verify or to establish the trust.
- When the receiver gets the CA he then decrypts it with the, sender's public Key.
- The browser when installed from scratch has a bunch of preloaded certificates.
- In cryptography, a **certificate authority** or **certification authority** (CA) is an entity that issues digital **certificates**. A digital **certificate** certifies the ownership of a public key by the named subject of the **certificate.**
- Anyone can slip or edit a certificate, into a machine.
- Revoking their certification is possible, but difficult

Governments inserting their own certificates into their countries laptops.
Deep packet inspection, by compromising the certificate store they are able to destroy PKI and reduce trust in the system

Bruce Schneier: 10 risks with PKIs

https://www.schneier.com/academic/paperfiles/paper-pki-ft.txt

1. Who do we trust, and for what?
2. Who is using my key?
3. How secure is the verifying computer?

4. Which John Robinson is he?
5. Is the CA an authority?
6. Is the user part of the security design?
7. Was is one CA or a CA plus a Registration Authority?
8. How did the CA identify the certificate holder?
9. How secure are the certificate practices?
10. Why are we using the CA process anyway?

- With web browsing, we are often only authenticating a URL. There's every chance the person or company we want to communicate with is not the URL we are authenticating.
- A potential issue is also found in the business side of CAs: the benefits of authentication are for the end user, but the costs for vetting website owners are borne by the CA. Therefore, are low cost CAs trustworthy? Who decides which CAs are included with browsers? - The browser publisher, but they might also receive payments from CAs that want to be listed.

SSL - Secure Sockets Layer

- Protocol that manages server authentication, client authentication and encrypted communication between clients and servers.
- if a webpage requires an SSL connection, the URL will change from HTTP to HTTPS and a padlock icon appears in the browser once the server has been authenticated.
- **Typically, an SSL certificate will contain:**
    - your domain name
    - your company name
    - your address, your city, your state and your country
    - the expiration date of the certificate
    - details of the Certification Authority responsible for issuing the certificate

TLS - Transport Layer Security

- Protocol that ensures privacy between communicating applications and their users on the Internet
- When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to SSL.

How it works

1. First, the web server sends the user a Certificate, which is a public key that has been signed by an authority.
2. The client then verifies the certificate using the public keys in your trust store.
3. Now that They've authenticated each other, they can start doing Diffie Hellman with confidentiality as they're on a secured connection.

4. The user first encrypts their number with the public key that the web server sends them.
5. The Web server then signs their number with their private key.
6. Once they're exchanged, both parties can use that generated shared Diffie Hellman Key to encrypt all the messages using AES.

HTTPS - HTTP over SSL or HTTP Secure

- Use of SSL or TLS as a sublayer under regular HTTP application layering
- Encrypts and decrypts user page requests as well as the pages that are returned by the Web server
- Protects against eavesdropping and man-in-the-middle attacks.

Perfect Forward Secrecy

- If our encrypted traffic is being observed and the observers manage to figure out the shared secret at some point in time, wouldn't it be nice to have an algorithm that ensures the safety of all past communications? This is perfect forward secrecy.
- HTTPS for example:
    - *Session key* and symmetric cipher for perfect forward secrecy
    - Uses PKI asymmetric cryptography and authenticate and setup a communication stream.
    - Then the server and client use this secure infrastructure to generate a symmetric session key, for example by Diffie-Hellman, that is tossed at the end of each session.
    - So a new key is used for every session.
    - MAC for integrity

Address Resolution Protocol and Cache Poisoning

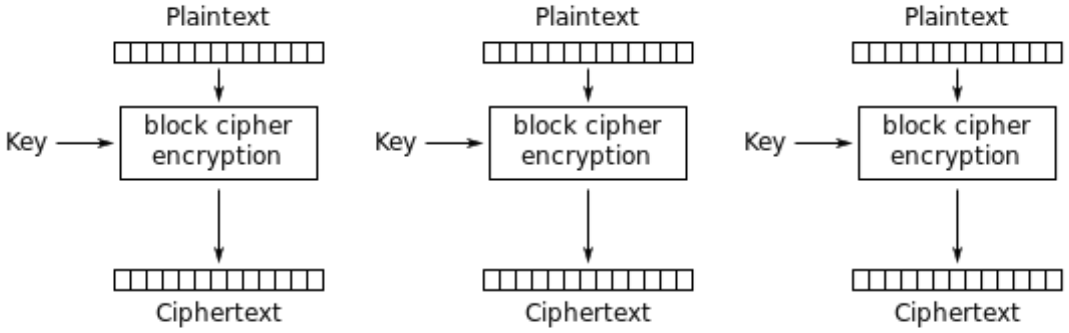
- ARP (Address Resolution Protocol) works out which devices (by MAC address) sit on which IP addresses on your local network, stored in ARP tables.
- ARP tables are stored on the switches for the network, but these caches can be 'poisoned' with fake entries.

Block Modes

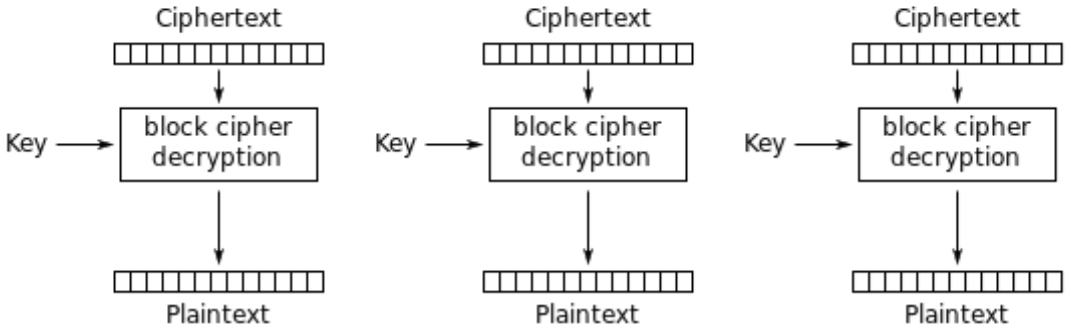
- When encrypting large amounts of data, the data is split up into chunks (blocks) and encrypted, then combined together to form the ciphertext. Block modes are the ways this can be done
- 3 methods
    1. ECB (Electronic CodeBook)
    2. CBC (Cipher block Chain)
    3. CTR (counter)

Electronic Codebook (ECB)

- Message is broken into 3 chunks
- Encrypt them independently
- Concatenate each ciphertext
- If two blocks are identical, then their ciphertexts will be identical. (See the fuzzy penguin)



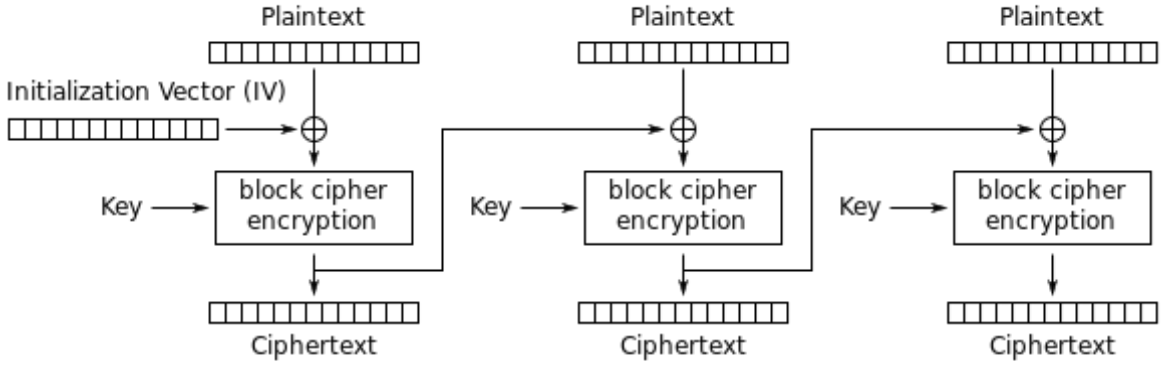
Electronic Codebook (ECB) mode encryption



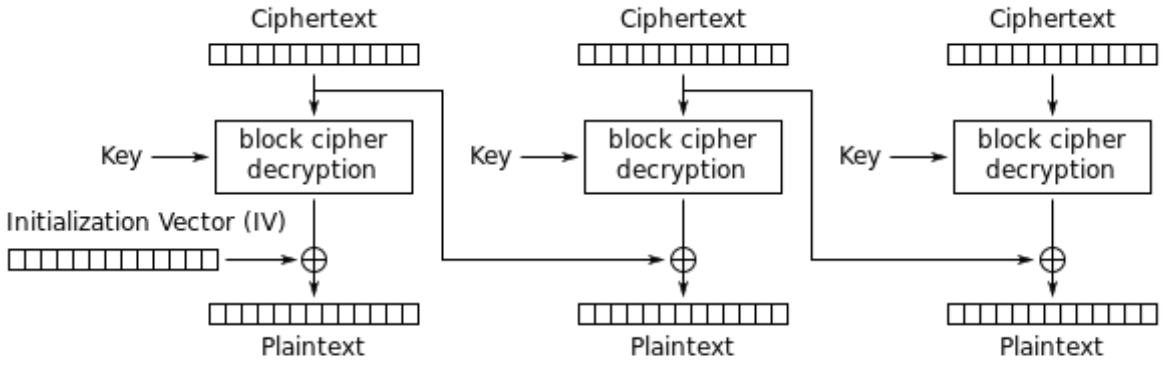
Electronic Codebook (ECB) mode decryption

Cipher Block Chaining (CBC)

- The plaintext is XORed with the previous ciphertext block before being encrypted
- The first block is encrypted using an initialisation vector (IV) which is sent in the clear
- Encryption is in series but decryption is parallel.
- Problems
    - When encrypting, each block can only be encrypted once the previous block has been encrypted (non-parallelised)
    - The message must be a multiple of the cipher block size
        - Vulnerable to padding oracle attacks
    - When decrypting, if the wrong IV is used on the first block, it becomes corrupted, however each subsequent block will be correct. This is because it uses the previous ciphertext to XOR



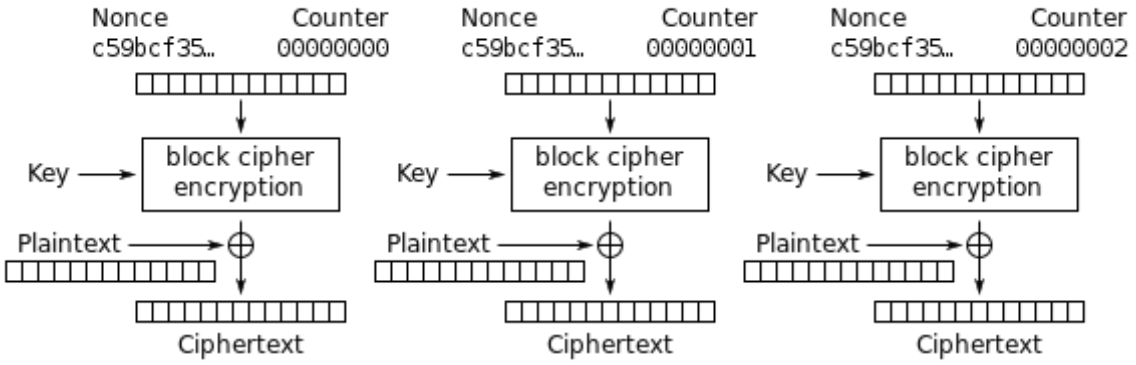
Cipher Block Chaining (CBC) mode encryption



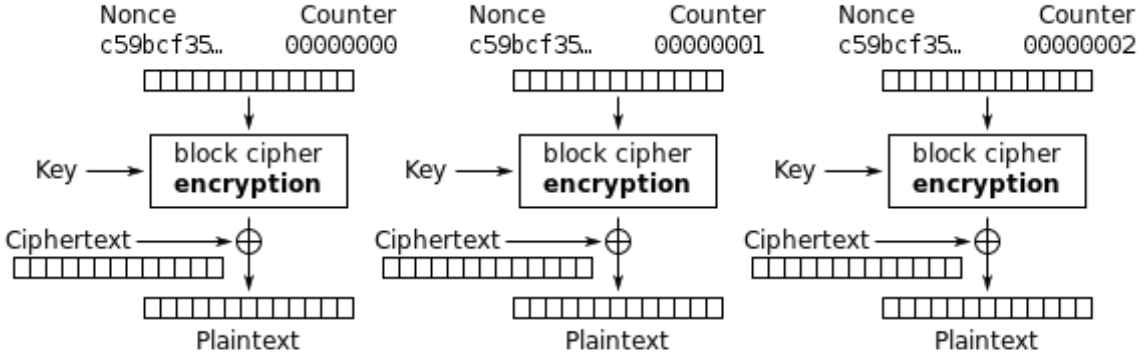
Cipher Block Chaining (CBC) mode decryption

Counter (CTR)

- An IV/nonce is combined with a counter using any lossless operation (concatenation, addition, or XOR) and encrypted.
- This is then XOR'd with the plaintext to obtain the ciphertext
- A few notes
    - The counter - can be any function which produced a sequence that is guaranteed not to repeat for a long time. Increment-by-one counters are the simplest and most popular
    - The IV/nonce
        - While it is better to be random it does not have to be
        - In the case of a non-random nonce (e.g. packet counter), the nonce and counter should be concatenated to maintain security
    - can be encrypted and decrypted in parallel as long as you have the nonce and counter for that block
- Problems
    - if non-random nonce is used and not concatenated with the counter it becomes very vulnerable to an attack



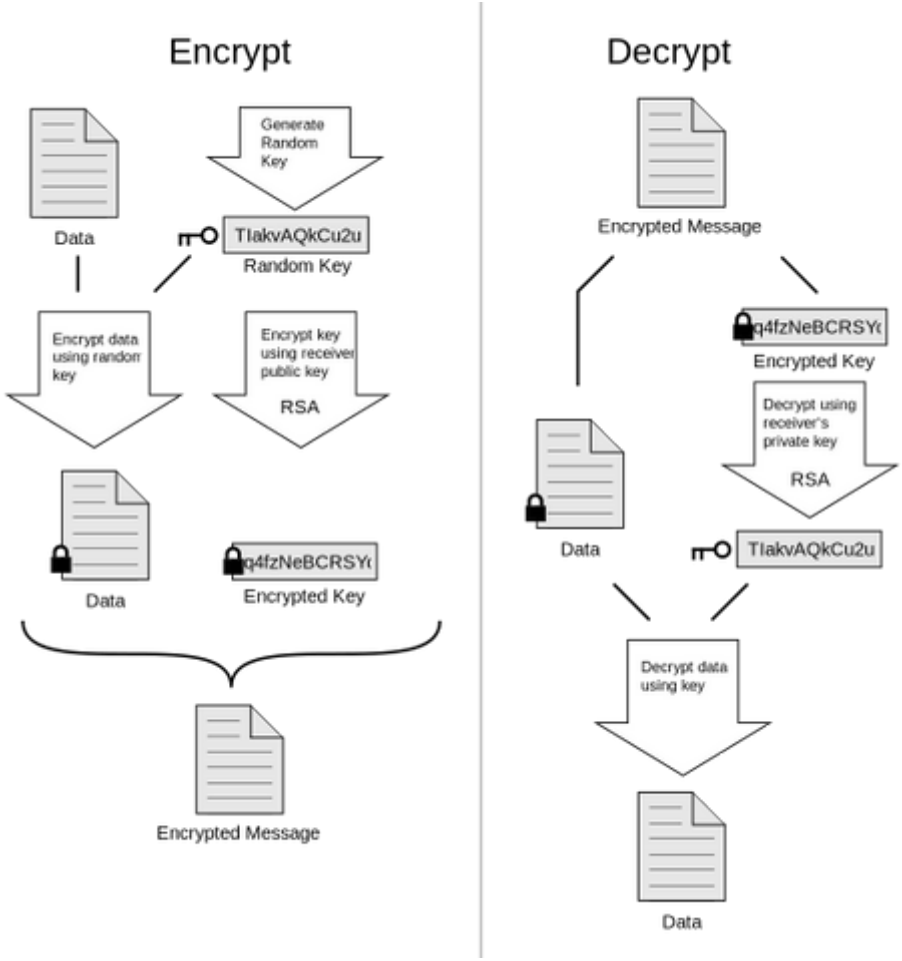
Counter (CTR) mode encryption



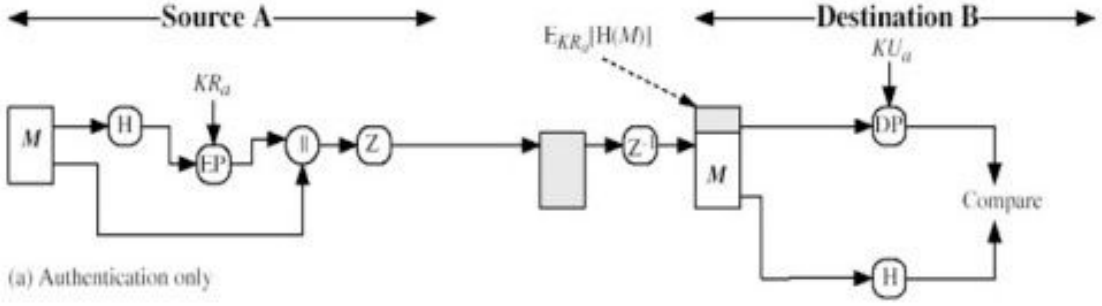
Counter (CTR) mode decryption

Pretty Good Privacy (PGP)

I don't believe this was explicitly covered in the lecture, but instead we were told to look it up in our own time.



- In the system, each user has encryption key publicly known, and a private key only known to user (like RSA).
- Since encrypting long messages using RSA can be time consuming, PGP uses a faster symmetric encryption method, and encrypts that key using the recipients public RSA key.
- It can be used as for authentication as follows:
    - A message (the information we want to receive, e.g. a website) is hashed to get a *message digest* and this is encrypted using the sender's private key to get a *signature*.
    - The signature is concatenated with the message and sent to the recipient. (In the diagram below, the *Z* is representing compression using a ZIP algorithm).
    - The recipient reverses this process using the public key of the sender to get the message digest, and hashes the message it received to ensure it matches the message digest meaning that the message authentically came from the sender.
- The weakness is that you have to be sure that the public key you're using belongs to the person you're trying to authenticate.



(a) Authentication only

MODULE #10

- In computing, time is not important. Sequencing is important, but not time. Time is abstracted away.
- But in security, time is very important, because claims are important.
- In the same way that race conditions can occur, it's important to say something before it's public knowledge, or proving that you said it before public knowledge.

WannaCrypt Discussion

- *WannaCry exploited 0-day flaws in Microsoft's software that were 'discovered' in April earlier this year. Microsoft had patched it up, but only in the later versions of software.*
- What would you do if you were in charge of an IT department and you started hearing things on the news about an attack such as WannaCrypt?
- Some of the ideas were:

PRE-ATTACK

- Continuously assess your systems
- Continuously update your software, though not even the latest version could be safe
- Keep a ransomware fund
    - BUT once someone knows that the fund exists and it runs out...
    - There is no guarantee that the attacker would give the data back
        - but if they don't give back the data, they lose authenticity, which means no one would pay

POST-ATTACK

- Immediately examine your systems to determine if they are vulnerable.
- Disconnect from the internet and backup your data.
    - Disconnecting your systems from the internet might be deemed to be an overreaction if you later find out that you ran a version of software that wasn't vulnerable.
    - The loss of business from disconnecting yourself from the internet may also be significantly more than it would have cost just to have paid the ransom if you did happen to be hit.
- Do nothing and have a beer.

These led on to the statement from Richard that **"in the early days of an attack no one really knows exactly what needs to be done and what systems are vulnerable."**
How do you determine if your system is vulnerable if the attack is only starting to unfold and the details aren't known?
A measured response is needed, however what is a measured response?

TOCTOU - Time of check, time of use error (see module 8).

Commitments

- A commitment is the process of providing something to a receiver (verifier) such as an encrypted file or a hash. We have committed to something which we can choose to open later (they cannot open without your permission) before a certain point in time.

Arbitrariness protocol

Arbitrariness protocol is a protocol without a trusted party.

- For example, the method for splitting a cake evenly between two people, because it's in both of the parties' interest to do so
    - The first person cuts a slice, the second person picks their slice.

How do you convince someone you know something in the past?

- Trusted third parties
- Salted hashes - Creating a hash with the country's name and a poem, and you reveal the poem afterwards.
- Isolating a person until after the event
- Proving you have power with other examples
- Encryption/Decryption doesn't work as you could have different encryption keys that decrypt to different things
- Ideally, we want to be using 0KP (zero knowledge protocol)

Proving knowledge

Protocol to prove that I knew who will win Eurovision next year, but I don't want you to know now:

- Write it down myself and then give you the paper next year (no..)
- Write it down and give it to you, you promise to not look (no..)
- Encrypt it into one-time hash
- Hash it with something additional, e.g. HASH(poem + winner name), and by next year give the poem, so the person can verify by hashing it.
    - This is called a **commitment**
- Tell the method of arriving to the name of the winner
- Demonstrate the power of predictions:
    - The authentication might get carried, when it's no longer true

Zero Knowledge proofs

a **zero-knowledge proof** or **zero-knowledge protocol** is a method by which one party (the *prover*) can prove to another party (the *verifier*) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true.

Examples

- I want to prove that I have a solution to a mathematical problem without leaking data about the solution. I.e. I want to prove to you that I know this piece of information without letting you know anything about this information/solution at all. (You know that I have it, you don't know what it is)
- In order to proof I have knowledge of a graph I would either provide an isomorphism of the graph or a hamiltonian cycle of the graph.

Exam Question Example

SCENARIO: Richard promised students that an exam would be easy. The students wanted him to prove it by showing them the exam.
PROOF:

- Have a container of 30 exam questions
- The students picked 20 questions out of the container
    - The remaining 10 questions became the exam.

This achieved the proof because any of the questions could have been in the exam, so it is accepted that they were all of the stipulated difficulty. As the students could see 20 of the questions, they could also judge their difficulty and decide if they were easy, but the actual exam questions weren't revealed to the students.

Maze Example

SCENARIO: Consider a maze with trillions of paths. The prover wants to show they know how to solve the maze.
PROOF:

- Prover picks a point and asks, "do you want a path from the start to the point, or a path from the point to the end."
- Verifier chooses path type and prover shows path.
- This is repeated until the verifier is convinced that the prover knows the path from the start to the finish.

House Burglar Example

SCENARIO: A burglar wants to prove that they can break into any house in a city
PROOF:

- The burglar builds a replica house from anywhere in the world
- Either show the verifier how to break into the replica house
    - The burglar can break into this house, since he/she built the house
- OR the real house in the city
- The verifier's trust in the burglar's statement builds up, and eventually the verifier is convinced the prover can burgle any house
    - BUT each time the verifier makes a choice, the chances of he/she being tricked by the burglar decreases
    - P(tricking the verifier for the first time) = 1/2
    - P(tricking the verifier a second time) = (1/2)^2
    - P(tricking the verifier a third time) = (1/2)^3
    - and so on.

One way of showing that you have a 0KP is to engage with someone who doesn't know any information and see if you get the same information as someone who does know.

Imagine Zero Knowledge Proof is like talking to a Ghost

More on Zero Knowledge Proofs

In cryptography, a **zero-knowledge proof** or **zero-knowledge protocol** is a method by which one party (the *prover*) can prove to another party (the *verifier*) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true.
If proving the statement requires knowledge of some secret information on the part of the prover, the definition implies that the verifier will not be able to prove the statement in turn to anyone else, since the verifier does not possess the secret information. Notice that the statement being proved must include the assertion that the prover has such knowledge (otherwise, the statement would not be proved in zero-knowledge, since at the end of the protocol the verifier would gain the additional information that the prover has knowledge of the required secret information). If the statement consists *only* of the fact that the prover possesses the secret information, it is a special case known as *zero-knowledge proof of knowledge*, and it nicely illustrates the essence of the notion of zero-knowledge proofs: proving that one has knowledge of certain information is trivial if one is allowed to simply reveal that information; the challenge is proving that one has such knowledge without revealing the secret information or anything else.
For zero-knowledge proofs of knowledge, the protocol must necessarily require interactive input from the verifier, usually in the form of a challenge or challenges such that the responses from the prover will convince the verifier if and only if the statement is true (i.e., if the prover does have the claimed knowledge). This is clearly the case, since otherwise the verifier could record the execution of the protocol and replay it to someone else: if this were

accepted by the new party as proof that the replaying party knows the secret information, then the new party's acceptance is either justified—the replayer *does* know the secret information—which means that the protocol leaks knowledge and is not zero-knowledge, or it is spurious—i.e. leads to a party accepting someone's proof of knowledge who does not actually possess it.
Some forms of non-interactive zero-knowledge proofs of knowledge exist,but the validity of the proof relies on computational assumptions (typically the assumptions of an ideal cryptographic hash function).

Homework:
How can you show that 2 large graphs are isomorphic using a zero knowledge proof?

Phishing Attacks

Spear phishing

Phishing attempts directed at specific individuals or companies have been termed **spear phishing**. Attackers may gather personal information about their target to increase their probability of success. This technique is by far the most successful on the internet today, accounting for 91% of attacks.

Clone phishing

Clone phishing is a type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original. This technique could be used to pivot (indirectly) from a previously infected machine and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email.

Whaling

Several phishing attacks have been directed specifically at senior executives and other high-profile targets within businesses, and the term **whaling** has been coined for these kinds of attacks. In the case of whaling, the masquerading web page/email will take a more serious executive-level form. The content will be crafted to target an upper manager and the person's role in the company. The content of a whaling attack email is often written as a legal subpoena, customer complaint, or executive issue. Whaling scam emails are designed to masquerade as a critical business email, sent from a legitimate business authority. The content is meant to be tailored for upper management, and usually involves some kind of falsified company-wide concern. Whaling phishers have also forged official-looking FBI subpoena emails, and claimed that the manager needs to click a link and install special software to view the subpoena.

Link manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email (and the Spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers. In the following example URL, http://www.yourbank.example.com/, it appears as though the URL will take you to the *example* section of the *yourbank* website; actually this URL points to the "*yourbank*" (i.e. phishing) section of the *example* website. Another common trick is to make the displayed text for a link (the text between the <A> tags) suggest a reliable destination, when the link actually goes to the phisher's' site. Many desktop email clients and web browsers will show a link's target URL in the status bar while hovering the mouse over it. This behavior, however, may in some circumstances be overridden by the phisher. Equivalent mobile apps generally do not have this preview feature.
A further problem with URLs has been found in the handling of internationalized domain names (IDN) in web browsers, that might allow visually identical web addresses to lead to different, possibly malicious, websites. Despite the publicity surrounding the flaw, known as IDN spoofing or homograph attack, phishers have taken advantage of a similar risk, using open URL redirectors on the websites of trusted organizations to disguise malicious URLs with a trusted domain. Even digital certificates do not solve this problem because it is quite possible for a phisher to purchase a valid certificate and subsequently change content to spoof a genuine website, or, to host the phish site without SSL at all.

Filter evasion

Phishers have even started using images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing emails.However, this has led to the evolution of more sophisticated anti-phishing filters that are able to recover hidden text in images. These filters use OCR (optical character recognition) to optically scan the image and filter it. Some anti-phishing filters have even used IWR (intelligent word recognition), which is not meant to completely replace OCR, but these filters can even detect cursive, hand-written, rotated (including upside-down text), or distorted (such as made wavy, stretched vertically or laterally, or in different directions) text, as well as text on colored backgrounds.

Website forgery

Once a victim visits the phishing website, the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original bar and opening up a new one with the legitimate URL.
An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge. Just such a flaw was used in 2006 against paypal

A Universal man in the middle attack(MITM) Phishing Kit, discovered in 2007, provides a simple-to-use interface that allows a phisher to convincingly reproduce websites and capture log-in details entered at the fake site.
To avoid anti-phishing techniques that scan websites for phishing-related text, phishers have begun to use Flash based websites (a technique known as phlashing). These look much like the real website, but hide the text in a multimedia object.

Covert redirect

Covert redirect is a subtle method to perform phishing attacks that makes links appear legitimate, but actually redirect a victim to an attacker's website. The flaw is usually masqueraded under a log-in popup based on an affected site's domain. It can affect OAuth 2.0 and OpenID based on well-known exploit parameters as well. This often makes use of open redirect and XSS vulnerabilities in the third-party application websites.
Normal phishing attempts can be easy to spot because the malicious page's URL will usually be different from the real site link. For covert redirect, an attacker could use a real website instead by corrupting the site with a malicious login popup dialogue box. This makes covert redirect different from others.
For example, suppose a victim clicks a malicious phishing link beginning with Facebook. A popup window from Facebook will ask whether the victim would like to authorize the app. If the victim chooses to authorize the app, a "token" will be sent to the attacker and the victim's personal sensitive information could be exposed. These information may include the email address, birth date, contacts, and work history. In case the "token" has greater privilege, the attacker could obtain more sensitive information including the mailbox, online presence, and friends list. Worse still, the attacker may possibly control and operate the user's account. Even if the victim does not choose to authorize the app, he or she will still get redirected to a website controlled by the attacker. This could potentially further compromise the victim.This vulnerability was discovered by Wang Jing, a Mathematics Ph.D. student at School of Physical and Mathematical Sciences in Nanyang Technological University in Singapore.Covert redirect is a notable security flaw, though it is not a threat to the Internet worth significant attention.

Social engineering

Users can be incentivised to click on various kinds of unexpected content for a variety of technical and social reasons. For example, a malicious attachment might masquerade as a benign linked Google doc.
Alternatively users might be outraged by a fake news story, click a link and become infected.

Phone phishing

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts.Once the phone number (owned by the phisher, and provided by a voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice phishing)

sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organisation. SMS phishing uses cell phone text messages to induce people to divulge their personal information.

Other techniques

- Another attack used successfully is to forward the client to a bank's legitimate website, then to place a popup window requesting credentials on top of the page in a way that makes many users think the bank is requesting this sensitive information.[41]
- Tabnabbing takes advantage of tabbed browsing, with multiple open tabs. This method silently redirects the user to the affected site. This technique operates in reverse to most phishing techniques in that it doesn't directly take the user to the fraudulent site, but instead loads the fake page in one of the browser's open tabs.
- Evil twin is a phishing technique that is hard to detect. A phisher creates a fake wireless network that looks similar to a legitimate public network that may be found in public places such as airports, hotels or coffee shops. Whenever someone logs on to the bogus network, fraudsters try to capture their passwords and/or credit card information.

Quantum Computing

There was a guest lecture by Matt McEwen on quantum computing.
Scott Aaronson is a computer scientist and wrote a book on quantum computing from a CS perspective.
It is available here for free http://www.scottaaronson.com/democritus/
IBM have a quantum computing experience that is available here
http://research.ibm.com/ibm-q/

MODULE #11

Trojan

Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a routine form to be filled in), or by drive-by download or from spam links and fake pop up & Advertisement. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity (IP address). Also, Ransomware attacks—which blocks access to data or threatens to publish it until a ransom is paid—are usually carried out using a Trojan.
Unlike computer viruses and worms, Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

Data corruption

Data Corruption refers to errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data. Computer, transmission, and storage systems use a number of measures to provide end-to-end data integrity, or lack of errors.
In general, when data corruption occurs a file containing that data will produce unexpected results when accessed by the system or the related application. Results could range from a minor loss of data to a system crash. For example, if a document file is corrupted, when a person tries to open that file with a document editor they may get an error message, thus the file might not be opened or might open with some of the data corrupted (or in some cases, completely corrupted, leaving the document unintelligible). The image to the right is a corrupted image file in which most of the information has been lost.
Some types of malware may intentionally corrupt files as part of their payloads, usually by overwriting them with inoperative or garbage code, while non-malicious viruses may also unintentionally corrupt files when it accesses them. If a virus or trojan with this payload method manages to alter files critical to the running of the computer's operating system software or physical hardware, the entire system may be rendered unusable.
Some programs can give a suggestion to repair the file automatically (after the error), and some programs cannot repair it. It depends on the level of corruption, and the built-in functionality of the application to handle the error. There are various causes of the

Incident Response

Hindsight is an easy thing to have. Looking back at the Lindt Siege, there wasn't very good planning prior to the situation occurring. Plans are important and should be made before an event. There should not be the assumption that a system is 100% secure, because it's definitely not.

With their being so many disasters in human history we should learn from them. The best way to learn is from mistakes, but lets learn from other peoples' not our own.
Incidents don't only happen in the physical world, but also happen digitally:

- Data breaches
- Malware outbreaks
- Denial of service attacks

The best way of learning is from mistakes, and the best mistakes are other people's mistakes.

Incident Response Example (Natural Disaster Tute Question)

Myself

Assets:

- Myself
- My Peers
- Friends and Family

Threats:

- Building collapse
- Water
- Longer-term threats (lack of food and drinking water)
- Short-term threats (panic)

Actions:
The correct action depends on the situation, however, it should always be possible to make an intelligent and worthwhile contribution to the incident response. Immediate threats should be prioritized; is anyone still left inside? Are there ways I could assist in calming people who are panicking? There may be people present who do not believe a natural disaster has occurred. Could an official be notified of this? People always believed those with authority.

The next action might be to contact friends and family. If this is done quickly, it may be possible to do this before the mobile network goes down. A longer term plan should also be set in motion for the scenario where leaving campus becomes impossible. A joint effort could be conducted to collect medical supplies for those that need them, and to collect a sufficient supply of food and drinking water to be rationed throughout the coming days.

Privacy

- Privacy is a rare and special thing. It has different properties to other things in security. It is very important these days, information is monotonically increasing. There is significant debate about government surveillance, with strong arguments on both sides, and probably no right answer.
- Richard suggests that we need perfect forward privacy. Is such a thing possible? How?

- **NSW Privacy Commissioner**
- Privacy refers to information and data. We have no law enshrining the right to be left alone. What privacy laws we do have were hard to pass, and no privacy laws exist in South Australia or Western Australia.
- The Privacy Commissioner is not a public servant, but is independent. This is important, as there could be possible conflicts of interest if she had to report up the chain of command.
- Privacy is not only good as a human right, but also has utilitarian value. For example, privacy tends to improve health outcomes.
- People from many backgrounds are useful in this field. Psychology, sociology, mathematics, etc.
- Facebook has a track record of bad privacy, and neither Richard nor the Privacy Commissioner use it. They do things like change their privacy policy without you having to agree to it.
- Many breaches in privacy occur due to engineering failures. Systems were not build robustly enough to protect privacy. We can and should do better.
- Privacy is a human right. It is an issue of human dignity. All cultures and societies value privacy in some way. People are currently not concerned enough about this.

Other

The issue with privacy - once information is out, it can never be taken back.

- Project Angelfire - camera system that captures views of entire cities. Used to track and backtrack perpetrators.
- Shopping centers/airports track your face, your location (from when you swipe your credit card), parking tickets, from your phone (bluetooth, MAC address), CCTV, etc.
- Henrietta Lacks - HELA cells: who owns her cells? Should she (+her family)?

MODULE #12

Whistleblowers

- People who expose any kind of information or activity that is deemed illegal, unethical, or not correct within an organisation that is either private or public
- Consequences of whistleblowing
    - Often information revealed about powerful organisations, thus you become a target for powerful people
    - Normally there are attempts at distracting or discrediting from the information
    - Personal attacks on the whistleblower, their credibility will start to be questioned
- Australia has really poor protections for whistleblowers
- Your own security and opsec is worth keeping in mind if you plan on doing any whistleblowing yourself
- The Whistleblower's Handbook by Stephen M. Kohn is a book worth reading

Exam details

- Three hour exam
- Normal stream only do Parts A and B, extended stream do Part C as well
- Part A - short answer and multiple questions, similar to examples posted online
- Part B - analysis
    - Four analysis questions to choose from
    - Normal stream have to select three of them to do, extended stream have to select two
    - One of the questions will be based on San Andreas (2015), a film voted on by the class
    - Similar to analysis done during tutorials and for case studies
    - One of the questions could be based on the pre reading done for case studies
    - Don't have to worry about little details like remembering statistics or what your actual "answer" is - these questions are posed to check your level of analysis and justifications for any answers you give
- Part C (extension students only) - practical exam
    - Have to answer two questions based on the extended topics (may get to choose from more than two, but will only have to write answers for two)
    - Definitely a question on format strings and padding oracles
- You will be given a digital copy of the textbook which you'll be able to use text search with
- **There'll definitely be an RSA question you'll need to work through**
- Supplementary exam if you do badly (so long as you've put in a non-trivial amount of work throughout the semester)

Clarification about disaster case study

- Running to the top floor of the library in the event of a tsunami is the worst possible thing you could do
- You can listen to an audio recording of Richard responding to this question here
- Runup distance (maximum limit the water reaches above sea level) is at most 20m for a tsunami and in this areas of the world, it's only about 2m; UNSW is already 40m above sea level so there is no chance of a tsunami reaching here
- Most deaths don't occur in the event itself, most deaths occur after the event because of a lack of resources (e.g. water, food, sanitation); the best thing to do is collect resources
    - Figure out how navigable roads are, check traffic flows
- Tsunami isn't a certainty after an earthquake but buildings won't be stable after an earthquake
- Head inland
- For storms, they move erratically, can't just look it up or run away
- Don't rely on information about the government, can listen to suggestions and advice but don't blindly trust it as it may be unreliable or conflicting
- Identify where friends or family are
- Work out what your assets are, what you're trying to protect and what your biggest risk is

Revision

RSA

- Don't expect anyone to use Euclid's algorithm to find the key
- Expected to be able to brute force or factor when trying to figure out the decryption key
- (Encryption key * decryption key) mod m = 1, where m = (p-1)(q-1)
- **Prime numbers list up to 100**
    - 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97

Hash vulnerabilities

- Basic idea: plain text comes in, hash comes out

- Preimage attack - know hash, can you find the plaintext?
- Second preimage attack - knowing the plaintext and hash, can you find another plaintext with the same hash? Find a *particular* collision
- Collision attack (birthday attack) - can you find any two texts that give the same hash? Find *any* collision, *not* a particular collision

Bits of security

- Normally one bit of security difference between worst case and average case (i.e. on average, it will take half the amount of time as the worst case)
- If you're a defender, you want to know the average case
- If you're an attacker, you want to know the worst case
- If you're unsure which one you need to answer with, write at the beginning of your answer that you're assuming average case

Confusion and diffusion

- **Confusion** - trying to destroy the relationship between the key and the cipher text; each bit of the ciphertext should depend on several parts of the key
- **Diffusion** - changing one bit of the plaintext should (statistically) change about half of the bits of the ciphertext and vice-versa

Mandatory access controls

- Used to limit people that you don't trust
- **Chinese wall**, information can't move from A to B
- **Dual control systems** require multiple people to stuff up. e.g. the Wargames video clip.
- **Multi layered security**. Can't read up, Can't overwrite down.
    - Fails because it depends on no one ever changing roles.
    - Has human weakness, in that any weakness at the top flows down to everything else.
- A proof is only ever as good as its assumption
- **Role based security** is separated from the levels
- **White listing**, denied by default.

Rootkits (from lecture video)

- A rootkit are a collection of tools used to escalate privilege of root. Then you would try and hide all traces of what you have done.

- What capabilities would you like your rootkit to have? capabilities to gather data about you, capabilities to gather data about the environment, and capabilities to hide traces of yourself.
- User levels:
    - **Ring level 2**: User level
    - **Ring level 1:** Root
    - **Ring level 0:** Hyperviser rootkits sits above everything else and controls all instructions in the system
- Whoever gets there first and has physical access wins
- **Where would you put the rootkit?** If you put in the hard drive/disk and you modify some code then it can be detected. Rootkits should live memory and processing space. If the system is turned off then you will lose access. However, reduce the chance forensics will find the rootkit.

CASE STUDIES

Module 1 - Deepwater Horizon Disaster

On 20 April 2010 (you may recall it) the deepest deep-sea oil-well ever drilled experienced a massive catastrophe. On the very day that BP managers were on board the Deepwater Horizon Oil rig celebrating 7 unbroken years without a lost-time accident; a series of unfortunate events, bad decisions, dangerous actions and equipment and safety failures led to gas and oil pouring over the rig platform, igniting, exploding, and causing the rig to lose control and begin to drift. The drill pipe was ripped out, the safety shutoffs failed in numerous ways, and oil from the undersea field began to to spew unchecked into the ocean, which it continued to do for months.

A U.S. Judge said of BP "Its employees took risks that led to the largest environmental disaster in U.S. history." BP has spent more than $28 Billion on cleanup costs, and $42 Billion in criminal and civil settlements and payments to a compensation trust fund.

> *Wikipedia reports:*
> *On 20 April 2010, while drilling at the Macondo Prospect, an uncontrollable blowout caused an explosion on the rig that killed 11 crewmen and ignited a fireball visible from 40 miles (64 km) away. The fire was inextinguishable and, two days later, on 22 April, the Horizon sank, leaving the well gushing at the seabed and causing the largest oil spill in U.S. waters.*

An attempt was made to activate the blowout preventer, but it failed. The final defence to prevent an oil spill, a device known as a blind shear ram, was activated but failed to plug the well.

The resultant oil spill continued until 15 July when it was closed by a cap.

Question

The US president has asked you to head up a Presidential Inquiry into the Deepwater disaster.

You have been asked to consider the main lessons should be learned from the disaster and to produce a shortlist of recommendations for actions to be taken to prevent future disasters.

The government, the public and the oil industry all support the enquiry and are prepared to devote considerable resources to implement your recommendations.

State and justify your top recommendations. Give them in decreasing order of importance (i.e. most important first).

Module 2 - Houdini

Renowned stage magician Harry Houdini (1874-1926) was outraged by mediums after some of them attempted to con him during his despair at his mother's death. He became a passionate debunker of mediums, delighting in publicly exposing fakes and frauds.

Mediums are people who claim to be able to speak with the spirits of dead people, and at this time in history they were quite popular and many people, called spiritualists, believed their powers were genuine. For example, bizarrely, Arthur Conan Doyle, the author who created the very rational Sherlock Holmes, was himself a spiritualist.

People consulted mediums to communicate (or so they thought) with their deceased loved ones. Houdini hated these mediums - thinking they were unscrupulously taking advantage of people who were in grief.

One of his most famous attempts at debunking was with the remarkable medium "Margery" aka Mina Crandon (see the reading below).

> *Spiritualism is the belief that the spirits of the dead have both the ability and the inclination to communicate with the living.*
>
> *Spiritualism developed and reached its peak growth in membership from the 1840s to the 1920s, especially in English-speaking countries. By 1897, spiritualism was said to have more than eight million followers in the United States and Europe, mostly drawn from the middle and upper classes.*
>
> *Spiritualism flourished for a half century. Many prominent spiritualists were women. By the late 1880s the credibility of the informal movement had weakened due to accusations of fraud perpetrated by mediums*

Mediums and Channelers

Mina "Margery" Stinson Crandon (1888–1941) ranks as one of the most thoroughly investigated and controversial mediums of the twentieth century. Psychical researchers put the ever-cooperative woman in uncomfortable situations, encased her in awkward contraptions, and sometimes wound her in enough adhesive tape to make her look like a mummy. In spite of such laborious efforts to disprove the validity of her phenomena, Margery Crandon again and again materialized spirits and performed astounding feats of psychokinesis, or mind over matter.

Mina Stinson was born in Canada in 1888 and moved to Boston when she was quite young. In 1918, after an unsuccessful marriage, she became the wife of a senior Boston surgeon, Dr. Le Roi Goddard Crandon, whose family dated back to the Mayflower. They bought the

house at Number 11 Lime Street on Beacon Hill, and became popular in Boston society. Crandon was a highly respected instructor at Harvard Medical School, and Mina was known as a lady with a sharp and lively wit.
In 1923, Crandon became extremely interested in psychical research, and he convinced Mina and a number of their friends to begin to explore the possibilities of contacting the dead. The group began with the customary attempts at table-tipping and spirit raps, and Crandon was astonished when it became evident that Mina was a powerful medium. After a few sessions Mina's deceased brother Walter, who had died in a train crash in 1911, announced his presence as her spirit control and within a brief period of time he began speaking through Mina and demonstrating a wide variety of spirit phenomena. Walter, speaking in down-to-earth language, often colored with profanity, stated that it was his mission to perform the process of mind over matter, rather than delivering flowery inspirational messages from the other side.

Although Mina was regularly producing dramatic phenomena, attendance to the seances were by invitation only in order to protect Crandon's standing at Harvard. Within a few months after they had begun the private seances, the Crandons submitted to the first formal investigation of Mina's mediumship under the auspices of Professor William McDougall, head of Harvard's Department of Psychology, and a committee from the university. After five months of observation, the committee declared its opinion that the spiritistic mind over matter phenomena were produced through fraudulent means.

In November of 1923, J. Malcolm Bird (1886–1964) of Scientific American magazine attended one of the Crandons' seances and was impressed with the spiritistic manifestations he witnessed. At that time, Scientific American was offering a prize of $2,500 to anyone who could provide conclusive proof that psychic phenomena truly existed, and Bird asked Mina to submit to a series of their tests. The investigating committee for the magazine included Harry Houdini (1874–1926), Hereward Carrington (1880–1958), Dr. Walter Franklin Prince (1863–1934), Dr. D. F. Comstock, Dr. William McDougall (1871–1938), and J. Malcolm Bird, secretary of the committee. To protect Mina Crandon's social standing as the wife of a prominent Boston surgeon and Harvard professor, Bird gave her the pseudonym of "Margery," which is how she shall always be remembered in the annals of psychical research.

The tests began in January 1924 under the general supervision of Crandon. The strictest of control conditions were enforced to ensure that fraud of any kind, conscious or unconscious, on the part of the medium could not go undetected. The most controversial aspect of the tests has to do with the role of the famous magician Harry Houdini in the experiments. Houdini was outspoken in his declarations that he had exposed Margery as a fraud. The medium's defenders proclaim that the greatest myth in the history of psychical research is that Houdini caught Margery cheating and exposed her. On one point there is agreement: Houdini seemed determined to expose Margery as a fake by whatever means necessary.

During one night of tests, Houdini brought an electric doorbell into the seance room and said that he would challenge the spirit to ring it for the circle. Once Margery was in a trance state, a low voice, that of Walter, the medium's deceased brother and her spirit control, bemoaned

the presence of Houdini. "Still trying to get some publicity by haunting seance rooms, eh?" the spirit voice taunted the magician.

Walter then directed Malcolm Bird, secretary of the committee, to take Houdini's doorbell out of the room so that he might examine it and see what kind of trickery the magician had planned. Bird hesitated for a moment, then picked up the apparatus and left the room. When he returned a few moments later, Bird frowned in displeasure at the magician, accusing him of having placed pieces of rubber on the contact points of the bell so that it could not possibly ring. Houdini offered no defense of his actions, and he was admonished that dishonesty would do the committee no service.

The words of admonishment were scarcely out of Bird's mouth when the electric bell began to ring in vigorous spurts of clanging sound, and Walter's booming voice filled the seance room. "How does that suit you, Mr. Houdini?" the spirit control mocked.

Houdini's tricks to confuse Margery were methodically uncovered by the all-seeing spirit guide Walter, and the magician's attendance at the sessions in the medium's seance room became more and more infrequent. When the committee demanded that the magician make good his boast that he could duplicate all the effects that the medium had manifested during her seances, Houdini found that he had suddenly been called away on business.

The investigating committee from the Scientific American never seemed to exhaust their list of inventive tests by which they might challenge the abilities of the patient Margery. For one experiment, the medium allowed herself to be encased in a wooden compartment which would permit only her arms and legs to protrude. With her limbs grasped firmly by the researchers, Margery was still able to ring bells, snuff out candles, and set in motion rocking chairs on the opposite side of the room.

In order to better investigate the spirit voices that seemed to be under Margery's control, the committee carefully measured an amount of colored water that would easily fill her mouth. With her mouth full of the colored water, the voices of Walter and other entities were still able to speak freely and to answer all questions put to them. After the experiment's completion, the water was removed from the medium's mouth and remeasured. The color remained the same and the amount of water withdrawn varied not more than a teaspoonful.

The water test had not adequately impressed all the investigators, however, so they devised a balloon which could be placed in the medium's mouth and inflated while the seance was in progress. Once again, the voices were able to engage in free discourse, even though Margery's larynx was completely blocked off. A number of the spirit voices expressed their scorn with the feeble attempts that the investigators were making in an attempt to mute them.

Although Margery was always remarkably patient and good-humored regarding the tests that the committee devised, there were some overeager members among the researchers who did not return her good will. Before the research seances had begun, each of the investigators had signed an affidavit stating that none of them would touch the ectoplasm

that streamed forth from the medium's body, but on one occasion, a committee member seized the substance as it moved over his wrist. Margery emitted a terrible shriek of pain, and later she became ill and hemorraged for several days. Another time when she was in deep trance, a researcher drove a thick needle into her flesh. Although the medium did not flinch while entranced, she suffered greatly from the wound when she awakened. On still another occasion, Margery was badly burned by corrosive chemicals which a zealous investigator had designed for an experiment.

After six weeks of tests, the committee remained undecided as to the validity of the phenomena produced by Margery, but an enthusiastic J. Malcolm Bird began writing positive articles concerning the authenticity of the medium's abilities. When it seemed apparent that there was no general consensus accepting or rejecting Margery's mediumship as providing proof of survival, Houdini became furious, fearing that they were about to hand over the prize money of $2,500 to the Crandons. Because of his open and much publicized skepticism of spirit mediums and Spiritualists, Houdini felt that his very reputation as a master magician was being challenged and insulted, so he wrote his own report, Houdini Exposes the Tricks Used by the Boston Medium Margery, and had it published as a booklet in 1924. As should be obvious from the title, Houdini presented his own explanations of how each of the phenomena manifested by Margery had been accomplished through trickery. The angry magician even went so far as to accuse two of his fellow committee members, Hereward Carrington and J. Malcolm Bird, of having assisted Margery in perpetrating her fraudulent mediumship.

In spite of crude and careless acts on the part of certain members of the committee throughout the grueling tests, Margery Crandon retained her goodwill toward the persistent investigators and produced a remarkable variety of phenomena, ranging from breezes, raps, spirit writing in several languages, independent voice manifestations, apports, and the imprint of spirit fingerprints in paraffin. Many members of the committee made public declarations that Margery Crandon had control of forces beyond the present knowledge of twentieth-century science. Hereward Carrington went on record as stating that after attending more than 40 sittings with Margery he had arrived at the "…definite conclusion that genuine supernormal would frequently occur. Many of the observed manifestations might well have been produced fraudulently…however, there remains a number of instances when phenomena were produced and observed under practically perfect control."

Unfortunately for Margery and her many friends and supporters, it was discovered that a fingerprint that had been allegedly left in wax by Walter was found to be that of a Boston dentist, Dr. Frederick Caldwell, who admitted that he had given Margery a bit of wax in which his own print had been pressed. One such exposure of fraud could not prove that all of Margery's spirit phenomena had been produced as products of clever deception, as Houdini had declared, but the falsification of her spirit control's fingerprint caused the majority of researchers who had examined and tested her mediumship to decide that perhaps she had, after all, been too good to be true.

Mina Crandon herself remains a mystery. The most famous medium of the 1920s has become a martyr in the minds of Spiritualists, a courageous woman who submitted to test

after complex test for the sake of demonstrating the truth of survival after death. For psychical researchers, she stands as a classic example of a talented medium who, though capable of occasionally producing genuine phenomena, from time to time resorted to trickery. For the skeptics, she is simply another clever fraud who deceived the gullible until she was exposed by the harsh light of scientific investigation.

Mina Stinson Crandon died in her sleep on November 1, 1941. Although she was said to have spent her final years unhappy and disillusioned, tending to her husband during a long convalescence, then succumbing herself to illness, her supporters never ceased to remind her that her fame as a medium was known throughout the world.

THE STRANGE CASE OF "MARGERY"

Mina Crandon, best known as “Margery”, was a Boston medium who found herself embroiled in one of the most bitter controversies in American psychic research. Her followers claimed that she was one of the greatest mediums who ever lived, while her critics called her a fraud and blamed her for almost bringing paranormal research in America to an end. Her heyday came about during the decline of mediumship in America and perhaps for this reason, more blame has fallen on her than she deserves. Regardless though, she was perhaps the greatest rival of magician Harry Houdini as he was involved in his crusade against fraudulent mediums and their bitter sparring and debates almost damaged his career beyond recognition as well.

Mina Crandon was born in Ontario in 1888 and moved to Boston when she was 16. A few years after that, she married a local grocer named Earl P. Rand, with whom she had a son. They remained happily married until a medical operation introduced her to Le Roi Goddard Crandon, a prominent surgeon. She divorced Rand in 1918 and married Crandon a short time later.

Crandon had no psychic experiences early in life and in fact, had no interest in the spirit world at all until her husband became interested in the early 1920’s. One evening in May 1923, Dr. Crandon invited a number of friends to his home for a “home circle” meeting. The group gathered around a small table and soon had it tilting in response to the sitter’s questions. Crandon suggested that they each exit the room, one at a time, to see which individual was responsible for the paranormal activity. One by one, each of them left and the table continued to tilt -- until it was Mina Crandon’s turn to leave.

Surprisingly, a few days before, a psychic had told Mina that she possessed supernatural abilities and that she sensed a laughing young man was attempting to contact Mina from the spirit world. The young man turned out to be Mina’s brother, Walter, who had died in 1911 in a railway accident. He would soon become Crandon’s spirit guide and, along with his sister, would become famous all over the world.

In addition to the celebrity gained by Crandon's ethereal brother, Mina herself became well-known for her risqué and sometimes bizarre séances. It was not uncommon for her to hold sessions in the nude and according to some, she was especially adept at manifesting ectoplasm from her vagina. It was also rumored that she had affairs with some of her would-be investigators, thus silencing a few of her most vocal critics.

The first test of Mina's psychic abilities took place in July 1923 under the guidance of Gardner Murphy, William McDougall and a group of Harvard graduate students and professors. When it was over, McDougall tried unsuccessfully to get Crandon to admit to fraud. She refused.

The panel questioned the reality of Crandon's abilities and it is likely that she would have faded into obscurity if not for the contest that was sponsored by Scientific American magazine. The contest was conceived by J. Malcolm Bird, an associate editor of the magazine, and it promised a prize of $2500 to any medium who could show genuine psychic ability. The judges were Walter Franklin Prince, an American psychical researcher; Hereward Carrington, a popular occult writer; Daniel Comstock, who introduced Technicolor to films; William McDougall, a professor of psychology a Harvard University; and magician and escape artist Harry Houdini.

The investigation, while it got a lot of press, was essentially a disaster. It was soon noticeable to everyone that there was a lot of friction between Houdini and the supporters of Margery, including J. Malcolm Bird, who had been assigned to observe, organize and record the investigation. Bird wanted Houdini disqualified from the panel and proceeded to start the investigations without him. Soon, the committee was deadlocked. Carrington and Bird believed that some genuine phenomena was occurring in Margery's presence but the others refused to commit without Houdini's opinion. At Bird's urging, they eventually relented and began to consider awarding Margery the $2500.

Houdini was shocked and traveled to Boston to witness a séance for himself. What happened next remains shrouded in mystery -- although it is clear that Crandon did not trust Houdini and the magician himself had stated that he was determined to expose the medium as a fraud. During the sessions, Houdini claimed to have seen Margery performing a number of tricks like making noises with her feet and lifting objects which were said to have moved on their own. In spite of this, he did not expose her publicly and asked that more stringent tests be performed. It was rumored that Margery had somehow outwitted Houdini -- and rumors also flew that perhaps her powers were genuine after all.

The following month, Houdini placed the medium in a wooden box with a hole in the top for her head and holes on each side so that her hands could be held during her entire séance. According to reports from the session, Margery's spirit control, Walter, took such a dislike to Houdini that the top of the box was allegedly ripped off by an invisible force.

The séance continued the next evening and Margery was placed back in the box. Shortly after she went into her trance and her spirit guide came through, the committee asked that she ring the bell which had been placed in the box with her. Immediately, Walter (the spirit

guide) exclaimed that Houdini had done something to the bell so that it would not ring. An examination of the bell revealed that a piece of rubber had been wedged against the clapper so that it would not ring! However, there was no proof that Houdini has tampered with it.

A short time later, Walter also said that Houdini had placed a ruler inside of the box so that he could later accuse Margery of cheating. The ruler too was found and later, Houdini's assistant would say that he had been instructed to place it there in case Houdini could not find another way to prove she was a fraud. It certainly appeared that Houdini had been caught cheating and he was widely discredited for it, leading many to doubt the integrity of some of his earlier investigations. In this case, the committee scheduled further tests of Mrs. Crandon but they were later cancelled. The decision on Margery's abilities was split and because of this, the money was never awarded. Houdini further outraged the Crandon's and their supporters when he published a small book called Houdini Exposes the Tricks Used by the Boston Medium Margery. He was as adamant about the fact that Margery was doing nothing more than offering clever tricks as her supporters were that what she was doing was genuine.

In 1925, J. Malcolm Bird published a book which supported Crandon and as research officer of the American Society for Psychical Research, he was able to sway many other ASPR members to her side. They became her greatest supporters and devoted hundreds of pages in the ASPR journal to her séances.

It was during this period that Margery began to develop a highly unusual manifestation that made her even more widely known in Spiritualist circles. On the table in front of her during a séance would be placed two dishes, one containing hot water and the other cold. In the first dish was a piece of dental wax. When the wax was softened, it was claimed that Walter (spirit guide again) would make an impression of his thumb on it -- then the thumbprint was put into cold water to harden. While it could not be proved that the prints were actually those of Margery's dead brother, it was proven that they did not belong to anyone present at the séance.

Believers were enthralled by this new manifestation. It was almost as if the spirit was leaving a calling card, even better. This, along with the whole question of Margery's mediumship, caused a major upheaval in Spiritualist circles. Unfortunately though, the suspicion of fraud never left her and many became disillusioned when thumbprints supposedly impressed in wax by Crandon's ghostly brother Walter, were shown to be exact matches for the thumbprints of Crandon's dentist, Dr. Kerwin. Police experts testified that there could be no mistake in this. The ruse was discovered when E.E. Dudley, a former officer of the ASPR, began collecting thumbprints from every individual ever known to have attended one of Margery's séances. Thanks to this, "Walter" was demoted to the status of a disembodied voice only.

Many researchers today believe that some elements of the paranormal were present in Crandon's séances, but just what was genuine and what was not remain unknown. Crandon and her husband were known for baiting investigators and trying to fool them if possible. The ASPR sustained the greatest amount of damage in the case, as the Crandon's never seemed to care who believed them and who did not. Just what secrets did Mina Crandon hold? We'll never know, because she took them to her grave in November of 1941.

The Medium and the Magician

It was a tense and rather peculiar gathering that took place on July 23, 1924, at 10 Lime Street, an elegant four-story brick house in the Beacon Hill neighborhood of Boston. In a narrow room on the top floor, five distinguished men had come together to try to communicate with the dead. Their hostess–and guide to the spirit realm–was vivacious, 36-year-old Mina Crandon, who had in recent months become well-known to the public under a stage name of sorts: 'Margery the Medium.'

Margery greeted her visitors in a flimsy dressing gown, bedroom slippers, and silk stockings. This attire, which left little to the imagination, was intended to rule out the possibility of concealment or trickery. It may have had other effects on her male visitors. Margery's girlish figure, fashionably bobbed light-brown hair, and sparkling blue eyes combined to make her, in the words of one bedazzled admirer, 'too attractive for her own good.'

During the previous year, Margery had conducted dozens of similar gatherings, or séances, for some hundreds of impressionable friends and acquaintances. Seated around a wooden table in the pitch-black room, Margery and her fellow'sitters' experienced a wide range of unearthly happenings. Mysterious bumps and raps rang out. Strange flashes of light pierced the darkness. Sometimes a wind-up Victrola would stop and start of its own accord, or disembodied voices would call from the shadows. Once a live pigeon appeared in the room, seemingly conjured from thin air. Even the table itself became an active participant in the proceedings, rearing up on two legs or rising toward the ceiling. At one especially lively sitting, it pursued a visitor from the room and knocked him off his feet.

Each of these remarkable events was thought to offer proof of the validity of spiritualism, the belief that it is possible for the dead to communicate with the living through an earthly conduit known as a medium. 'I consider the psychic question to be infinitely the most important thing in the world,' declared Sir Arthur Conan Doyle, the creator of Sherlock Holmes and the world's most visible proponent of spiritualism. 'All modern inventions and discoveries will sink into insignificance beside those psychic facts which will force themselves within a few years upon the universal human mind.'

Conan Doyle was not alone in this view. Spiritualism had been on the wane for decades, but in the wake of World War I, as death touched tens of thousands of households on both sides of the Atlantic, the movement underwent a rebirth. Friends and relatives of fallen soldiers flocked to séances, desperate to receive some word or sign of 'life beyond the veil.' Many of

the mediums who set up shop during this period were obvious frauds, callously playing upon the hopes of the bereaved. Others, like Mina Crandon, were not so easily dismissed. Her astonishing versatility and personal charm soon propelled her to international fame, and sparked an enduring controversy.

To a large extent, that controversy began at Margery's July 23 séance. Up to this point, the medium had displayed her talents almost exclusively to sympathetic audiences, who readily saw evidence of their departed loved ones in the strange manifestations at Lime Street. On that particular night, however, the sitters were of a more critical frame of mind, none more so than the man seated to Margery's left–Harry Houdini.

Houdini, who had achieved world fame through his skills as a magician and his abilities as an escape artist, had been creating a new role for himself as the'scourge of spirit mediums.' 'I am willing to be convinced,' he wrote earlier that year; 'my mind is open, but the proof must be such as to leave no vestige of doubt that what is claimed to be done is accomplished only through or by supernatural power.'

Houdini's public crusade had its roots in a private grief. The death of his beloved mother in 1913 had been 'a shock from which I do not think recovery is possible.' In the intervening years he had attended hundreds of séances, but his longing to contact his mother soon turned to rage at the obvious deceptions he encountered. It galled him to see the public bilked by unscrupulous mediums whose talents, he thought, were no more supernatural than those of 'honest' magicians. He soon vowed to devote the remainder of his life to exposing fraudulent mediums. Even in this, the magician could not entirely restrain his flair for the dramatic. Often he attended séances wearing a false beard and mustache or some other camouflage, the better to observe without being detected. When he had gathered enough evidence to make an exposure, he would leap up, tear off his disguise, and shout, 'I am Houdini! And you are a fraud!'

Houdini needed no disguise when he called upon Margery; the medium relished the chance to convert such a notorious skeptic. Some observers saw this encounter as an acid test–not just of Margery's mediumship, but of spiritualism itself. But if Houdini truly maintained an open mind on the subject, as he often claimed, there was little evidence of it that night as the small séance room came alive with otherworldly activity. A spirit bell rang. A voice called to him in the darkness. A megaphone crashed to the floor at his feet. If these manifestations impressed him, he gave little sign. When the lights came back on, Houdini thanked his hostess and took his leave. On the drive back to his hotel, the magician gave voice to his true feelings. 'I've got her,' he declared. 'All fraud.'

Mina Crandon seemed an unlikely medium. Where the celebrated Helena Blavatsky, founder of the movement known as Theosophy, had been solid and serious, Mina Crandon resembled nothing so much as a light-hearted flapper. Even Houdini conceded that she was an exceedingly attractive woman, and one psychic researcher cautioned his colleagues to 'avoid falling in love with the medium.' The daughter of a Canadian farmer, Mina had moved to Boston as a teenager to play piano, cornet, and cello in various local dance bands and orchestras. After working as a secretary, an actress, and an ambulance driver, Mina

divorced her first husband and married Dr. Le Roi Goddard Crandon, a former instructor of surgery at the Harvard Medical School, in 1918. She was barely 30. Dr. Crandon was at least a dozen years older.

It was Dr. Crandon who introduced his wife to the paranormal. In the spring of 1923 he had become intrigued by an account of ‘table tipping,’ a rudimentary form of mediumship not unlike a Ouija board. Crandon ordered a table constructed to the exact dimensions specified in the book he had been reading. Toward the end of May, Crandon and his wife invited four of their friends to join them in an attempt to recreate the table-tipping experiment. Following Crandon’s terse instructions, the sitters took their places at the table, joined hands, and waited for some sign of a spirit presence.

Nothing happened. Mina began to feel silly. ‘They were all so solemn about it that I couldn’t help laughing,’ she recalled. ‘They reproved me severely, and my husband informed me gravely that ‘This is a serious matter.”

Then, abruptly, the table began to move–only slightly at first, but then more violently, tilting up on two legs before crashing loudly to the floor. Crandon demanded to know which of his guests possessed the mediumistic talent necessary to cause this manifestation. One by one, the physician instructed his friends to remove their hands from the séance table. The table stopped its rocking only when the last of the sitters lifted her hands. Dr. Crandon had his answer. The medium was his own wife.

At first, the very idea of being a medium seemed a great lark to Mina. All through the summer of 1923 the Crandons conducted one séance after another. In each case, Mina appeared to exhibit some strange new power. Indeed, it seemed that Dr. Crandon had only to read of some new psychic manifestation before Mina could duplicate it.

Within a month of the first séance, Dr. Crandon announced a plan to place his wife under hypnosis, in the hope of making contact with a ‘psychic control’ who would serve as her guide to the spirit world. At first Mina resisted this suggestion, claiming that she didn’t want to miss any of the ‘fun’ while under hypnosis. Eventually, however, she gave in to her husband’s wishes, and before long an unfamiliar male voice made itself known to the Crandon circle. ‘I said I could put this through,’ it announced.

The voice, it was thought, belonged to Walter Stinson, Mina’s older brother, who had been crushed to death in a railroad accident a dozen years earlier. From this point forward, Walter’s spirit was a regular presence in the séance room at Lime Street.

Walter proved to have a forceful personality. He had a quick and ready wit and was much given to rough language. Many visitors to the Crandons’ séance room became convinced of the truth of what they heard simply because they could not imagine that such coarse and irreverent language would issue from the lips of the demure doctor’s wife. ‘Hell is now completely up to date,’ Walter once quipped to a roomful of clergymen. ‘We burn oil!’

Several observers noted that Walter's voice did not appear to come from Mina at all. The sound seemed to originate in a different part of the room, and would continue unabated even while Mina snored her way through a hypnotic trance, or held her mouth full of water. The effect proved so remarkable that one skeptic, searching for some plausible explanation, wondered aloud if perhaps the lady could speak through her ears.

Believing his wife to be a 'remarkable psychic instrument,' Dr. Crandon took her abroad to build up a consensus of favorable opinion from European experts. One of these was Sir Arthur Conan Doyle, who declared her to be 'a very powerful medium' and that the validity of her gifts was 'beyond all question.'

J. Malcolm Bird, an associate editor of Scientific American magazine, shared Conan Doyle's opinion and wrote a series of articles extolling Mrs. Crandon's gifts. It was Bird who gave her the name 'Margery,' in an effort to protect the Crandons' privacy. Under this name, her renown steadily grew.

By bringing Mrs. Crandon to the attention of Scientific American, Conan Doyle had inadvertently placed her at the center of a growing controversy. In December 1922 the magazine had launched an investigation into the paranormal, with a cash prize of '$2,500 to the first person who produces a psychic photograph under its test conditions' and '$2,500 to the first person who produces a visible psychic manifestation of other character . . . to the full satisfaction of these judges.' A special investigating committee would examine all mediums who applied for the prize, with Bird acting as its secretary. Conan Doyle regretted that Bird, a Margery supporter, would have no investigative role, as the author harbored reservations about the rest of the committee, which included several skeptics. When Houdini was asked to lend his talents, Conan Doyle expressed outrage at the 'capital error' of placing an enemy of spiritualism on such a body. 'The Commission is, in my opinion, a farce,' he wrote.

The Crandons, for their part, seemed to welcome the opportunity to test Margery's mettle against the notorious Houdini. Though Scientific American's money meant little to the wealthy couple, the opportunity to win the approval of such a prestigious body–at Houdini's expense–proved too great a temptation to resist. Dr. Crandon wrote to Conan Doyle of his willingness to 'crucify' any investigators who doubted his wife. Even the discarnate voice of Walter, speaking from the spirit plane, appeared to relish the challenge.

As it happened, Houdini was not notified when the Scientific American committee began its investigations, and he didn't learn until three months later that the proceedings were under way at all. By this time, rumor had it that the committee was on the point of declaring Margery genuine and awarding her the prize. Bird, in particular, seemed eager to give the magazine's endorsement and allowed word of the favorable findings to find its way to the press. 'Boston Medium Baffles Experts,' announced one headline. 'Houdini the Magician Stumped,' declared another.

Houdini, who had not even been present at the investigation, much less stumped, was not pleased. He told Scientific American that he would forfeit $1,000 of his own money if he failed to expose Margery as a fraud. Traveling to Boston, he reviewed the findings of his

peers. To his way of thinking, the investigation had been mishandled from the start. Most of the committee members had availed themselves of the Crandons' generous hospitality during the proceedings–staying in their home, eating their food, and enjoying their company. This, Houdini believed, had badly compromised their objectivity. Later it was revealed that accepting room and board had been the least of the transgressions. One investigator had actually borrowed money from Dr. Crandon, while another hoped to win his backing for a research foundation. Worse yet, the distinguished panel was not unaware of Mrs. Crandon's attractions. At least one committee member drew comfort in his old age from the recollection of amorous encounters with the celebrated medium.

After the July 23 séance, Houdini left the Crandon home much impressed by the famous Margery–though not by any supernatural powers, he hastened to assure his colleagues. At his hotel later that evening, the magician explained how and why his conclusions differed from theirs. One feat that had baffled the other sitters was the ringing of a'spirit bell box,' a small wooden clapper-box that sounded an electric bell when pressed from the top. Although Margery's hands were held by the sitters on either side of her and her feet were in contact with theirs, the bell box rang repeatedly throughout the séance–a phenomenon she attributed to Walter.

Usually the bell box sat on the floor between Margery's legs, but Houdini had insisted that it be placed on the floor at his own feet. Despite this precaution, the bell rang as merrily as ever. Houdini had a ready answer: 'I had rolled my right trouser leg up above my knee,' he later wrote. 'All that day I had worn a silk rubber bandage around that leg just below the knee. By night the part of the leg below the bandage had become swollen and painfully tender, thus giving me a much keener sense of feeling and making it easier to notice the slightest sliding of Mrs. Crandon's ankle or flexing of her muscles….I could distinctly feel her ankle slowly and spasmodically sliding as it pressed against mine while she gained space to raise her foot off the floor and touch the top of the box.' In short, Margery's agile foot, not a spirit visitor, had been responsible for the ringing bell.

Another of the evening's mysteries had involved a megaphone that–according to the disembodied voice of Walter–had been levitated in the darkness above the sitters' heads. 'Have Houdini tell me where to throw it,' the voice had commanded.

'Toward me,' answered Houdini, whereupon the megaphone instantly crashed to the ground in front of him. Here, too, Houdini had an explanation. Earlier in the proceedings, he said, when one of Margery's hands momentarily came free, she had snatched up the megaphone and placed it on her head, like a dunce cap. In the total darkness of the séance room, no one would have seen her do this. Later, with both of her hands again under control, the medium had made the megaphone sail through the air simply by snapping her head forward. 'This,' Houdini acknowledged, 'is the 'slickest' ruse I have ever seen….'

To assure proper control at future séances, Houdini designed a special 'fraud-preventer' cabinet, a slant-topped crate with openings for the medium's head and arms. Once inside, Margery's movements–and the opportunities for deception–would be severely limited. Reluctantly, Margery agreed to conduct a séance from within the cabinet, but not before Dr.

Crandon and Houdini exchanged such harsh words that Walter himself felt compelled to call for a truce.

The first séance with the cabinet was not a success. Acting on a tip from Walter, Dr. Crandon discovered a small pencil eraser wedged into the bell box to prevent it from ringing. Outraged, the physician accused Houdini of attempting to sabotage the proceedings–a charge the magician repeatedly denied.

Another attempt proved even more dismal. A collapsible carpenter's ruler–which might have been used to manipulate the bell box and other apparatus from within the cabinet–was discovered at Margery's feet. Margery's defenders saw this as a craven attempt by Houdini to discredit her. 'Houdini, you God damned bastard, get the hell out of here and never come back!' exclaimed the voice of Walter at the séance. In Houdini's view, the folding ruler had been planted to impugn his testimony, and he resented that anyone would take Walter's word over his.

By the time Scientific American finally declined to grant the prize to Margery, in large part due to Houdini's exposures, the combustible magician had quarreled, sometimes violently, with every member of the committee. Bird, whom Houdini suspected of active collusion with the Crandons, had resigned as secretary. In his final verdict of the Margery phenomenon, Houdini wrote, 'My decision is, that everything which took place at the seances which I attended was a deliberate and conscious fraud….'

From the great beyond, Walter weighed in with a prediction: Houdini, he said, would be dead within a year. Houdini managed to thwart the prophecy, but only just. He died on October 31, 1926, of complications following a blow to the stomach. In an interview with the press, Margery offered a few words of conciliation, praising Houdini's virile personality and great determination.

Despite Houdini's exposures, Margery emerged from the debacle essentially unscathed. In the séance room, she went on to better things. By the end of 1924 she had begun to produce 'teleplasmic' manifestations similar to those of Eusapia Palladino, a famed Italian medium. Sitters were now treated to the sight of ectoplasm–said to be the substance of spirit emanations–issuing from Margery's nose, mouth, ears, and other body openings. The emanations, once extruded from the medium's body, sometimes formed themselves into the shape of crude hands. These ectoplasmic limbs, the medium claimed, were responsible for the ringing of the bell box and other phenomena.

Eric J. Dingwall, an officer of Britain's Society for Psychical Research, was one of the first to investigate Margery's latest wonder. Having evidently won the confidence of Walter, Dingwall was permitted to view the teleplasmic emanations by the light of a red lamp, which Dr. Crandon flashed on and off to reveal brief glimpses of the phenomenon. Too much light, Crandon explained, would have an inhibiting effect on the ectoplasm. 'The materialized hands are connected by an umbilical cord to the medium,' Dingwall wrote to a friend, 'they seize upon objects and displace them.' Later, when Dingwall was permitted to clasp one of

the teleplasmic hands, he described it as feeling like ‘a piece of cold raw beef or possibly a piece of soft wet rubber.’

Mid-way through his investigations, however, Dingwall began to entertain doubts. Dr. Crandon’s lamp never allowed him to see the ectoplasm actually extrude from Margery’s body; he had only seen it after the fact. Odder still, photographs revealed that many of the emanations appeared to be hanging from slender, almost invisible threads. Others who examined the photographs noted that the ectoplasm looked suspiciously like animal lung tissue, a substance Dr. Crandon might have obtained through his work at Boston hospitals. Dingwall’s final report on the matter was inconclusive.

Margery remained characteristically unconcerned. In an earlier age, she noted, she would have been executed as a witch. Now she found herself the subject of learned investigations. ‘That represents some progress, doesn’t it?’ she asked.

Sitters continued to file into the séance room at Lime Street. One investigation after another raised the possibility of fraud, but none seemed able to make the allegations stick. Even J.B. Rhine, later to become one of the driving forces of paranormal research, was intrigued by Margery, but he came away unimpressed by what he had seen. As ever, Conan Doyle defended the medium. When Rhine published an unflattering account of his experience with Margery, Conan Doyle bought space in several Boston newspapers to run a reply. The black-bordered message read simply: ‘J. B. Rhine is an ass.’

By 1928, Margery had added yet another effect to her repertoire, one that promised to excite even more speculation. In recent séances, Walter had hinted that it might be possible for him to leave behind a fingerprint. On a visit to her dentist, Dr. Frederick Caldwell, Margery asked if the hot wax used to take dental impressions might also be used to obtain Walter’s fingerprint. Caldwell demonstrated how well the wax preserved his thumbprint and gave Margery his sample print and all the necessary materials to make new ones.

That very night, Walter left a thumbprint in the wax. When a so-called fingerprint expert used by the Crandons said the print matched one taken from an old razor that once belonged to Walter Stinson, Margery appeared to have confounded the skeptics. Yet when psychic researcher E.E. Dudley set out to compare Walter’s wax print with those of people in the Crandon circle, he made a surprising discovery: Walter’s thumbprint was identical in every way to that of Margery’s dentist, Dr. Caldwell. Someone had apparently used the sample thumbprint Dr. Caldwell had made for Margery to create a metal die-stamp suitable for making impressions in wax. The ax had finally fallen. Even many devoted adherents backed away from their earlier endorsements. Malcolm Bird, once her staunchest defender, admitted that at times he had been guilty of elaborations and half-truths. The scientific community let it be known that Margery’s séances no longer held any interest.

The medium’s decline was rapid and tragic. With the death of Dr. Crandon in 1939, Mina grew melancholy and depressed and turned to alcohol for consolation. She began to look older than her years; one visitor described her as ‘an overdressed, dumpy little woman.’ She seemed to have difficulty controlling her emotions. During one séance the medium grew so

distraught that she climbed to the roof of the Lime Street house and threatened to throw herself off.

Mina Crandon died at the age of 54 in 1941. In the end she had been worn down not so much by the assaults of adversaries like Houdini, but by the entreaties of her supporters, who continually demanded new and better miracles from her. As Eileen Garrett, a fellow medium, observed, ‘Margery’s best friends were her worst enemies.’

Question

Houdini (correctly) anticipated that after his own death it was quite likely that unscrupulous mediums would try to pretend his spirit was in touch with them, and they would claim that Houdini was saying they were not fakes after all.
So to forestall them he publicly announced that he would try to contact his wife Bess via mediums after his own death, and then he **privately worked out a protocol with her** to prevent the mediums from claiming his "spirit" was telling them messages to pass onto Bess, when in fact they were just inventing the messages. In other words, to prevent the mediums from cheating and passing off false messages claiming they were from Houdini.
Sadly Houdini's actual protocol was flawed. Can you do better?
Suppose you are Houdini, and you need to devise the protocol to share with your trusted partner.

Q1. State and briefly justify the most important properties your protocol should have:
Q2. Give your protocol:

Module 3 - Doors on Planes

AirNZ Pilots stood down

Air New Zealand has stood down two pilots after midair "tension" between the pair led to the first officer being locked out of the cockpit.

The Captain involved in the incident has been taken off duty for two weeks and the First Officer for one week.

The incident occurred on a Perth-Auckland flight on May 21 following a delay in the flight's departure.

Air New Zealand says the flight was delayed after the first officer was required to undertake a random drug and alcohol test.

"This departure delay frustrated the captain who prides himself on operational efficiency," Air New Zealand's manager of operational integrity and safety Errol Burtenshaw said.

During the overnight flight the first officer left the flight deck for a comfort break before having coffee with a cabin crew member in the galley area.

When he tried to return to the cockpit the crew member spent up to two minutes attempting to call through to the captain to advise that the first officer was at the hijack secured cockpit door, but the calls went unanswered.

"The captain did not respond or open the door because he was approaching a navigational waypoint and in his cockpit monitor saw a cabin crew member rather than the first officer ringing," Mr Burtenshaw said.

"The first officer became concerned that the captain did not answer the calls and used an alternative entry method to gain access."

The airline has conducted an investigation into the incident and a report has been sent to aviation authorities.

Mr Burtenshaw said both pilots have undergone counselling and additional training.

The Civil Aviation Authority says it is satisfied with the disciplinary action.

Some cabin crew became anxious about the inability to contact the captain and were offered counselling.

Co-pilot deliberately crashed German Wings flight

The captain of the doomed Germanwings plane reportedly used an axe to break down the cockpit door in the final moments before his co-pilot “intentionally” descended the plane, German media has suggested.

Evidence from the cockpit voice recorder suggested the captain of the Airbus A320, who The Independent understands is named Patrick Sondenheimer, left the flightdeck mid-journey, presumably to go to the toilet. Prosecutors say he returned to find his co-pilot Andreas Lubitz had barricaded himself inside and had sent the plane into descent over the French Alps.

Sources told the newspaper he struck the door repeatedly up until the plane crashed into the mountain, possibly causing the banging sounds heard on the cockpit voice recorder.

Germanwings has confirmed that an axe was on board for safety reasons, as is routine on all Airbus A320 models. Investigators would not comment on whether it was used to gain entry to the cockpit.

The President of France's pilot union has since claimed the axe would have been kept in the cabin, telling BMFTV: "The only tools available in the cabin are crowbars."

The only sound heard from inside the cockpit is steady breathing, implying Lubitz was alive until the moment of final impact.

Pilot opens toilet door with axe

A Swedish pilot had to prise open a toilet door with an axe, after a drunk passenger refused to leave the cubicle.
The man, who was in his 50s, locked the bathroom door 10 minutes before the Nextjet's flight from Stockholm was due to land in the northern town of Ornskoldsvik on Wednesday.
He was repeatedly asked to return to his allocated seat in order to comply with safety regulations.
But he refused to co-operate, prompting the captain to intervene.
He grabbed the axe and used it to pry open the door so he could remove the man.
"He definitely did not smash down the door, it's not as dramatic as one might think," police chief Kerstin Svedberg told AFP.
The passenger was not taken into custody, but is suspected of violating Swedish aviation laws.
He could face a fine or up to six months in prison if convicted.

AirIndia Pilot locked out of cabin when door jams

An Air India flight was forced to land after the pilot was locked out of the cockpit during a toilet break, the airline says.
He was unable to gain access to the cockpit because of a jammed door.
Flight AI 403, which was travelling from Delhi to Bangalore, was diverted to Bhopal Airport on Monday.
The airline has been plagued by financial difficulties in recent years, with its 787 Dreamliner jets grounded in January by safety concerns.
"The commander of the flight had left the cockpit for a short while to visit the toilet and on returning to the cockpit found the door locked. The door had got jammed and all efforts to open the door, even from inside by the co-pilot, failed," an Air India statement said.
"The co-pilot, after taking permission from ground control, diverted the flight to Bhopal and landed...at 17:55 hrs."
The door was fixed by ground maintenance engineers and the plane continued its journey less than three hours later, Air India adds.
Stewardesses
The state-run airline is currently investigating a separate incident in which the auto-pilot system of an Airbus 321 flying from Bangkok to Delhi on 12 April was accidentally switched off.

According to the Mumbai Mirror, two pilots had taken a 40-minute break from the cockpit and left two stewardesses in their seats to operate the plane in their absence.
One of the stewardesses accidentally turned off the auto-pilot, forcing the pilots to rush back to their seats, the report said.
Air India has denied this account but said cabin crew did "overstay" in the cockpit and that the autopilot was briefly disconnected "due to distraction".
Meanwhile, Civil Aviation Minister Ajit Singh said on Tuesday that all six of Air India's Boeing 787 Dreamliner passenger jets would resume flying by the end of May, starting with a domestic flight on Wednesday.
The planes have been grounded worldwide since the beginning of the year over a string of incidents, including fuel leaks, a cracked cockpit window, brake problems and an electrical fire.
However, it is overheating in batteries providing auxiliary power that has caused the most concern.
Mr Singh also said he expected the airline to make a net loss of about 40bn rupees ($730m) for the current financial year ending March 2014, compared with about 52bn rupees in the previous year.

Question

You are the amazing Dick Smith. Skeptic, philanthropist, all round nice guy, and former Chairman of the Civil Aviation Safety Authority Board.

In light of the German Wings incident and the earlier EgyptAir incident the Civil Aviation Safety Authority, the government statutory authority responsible for the regulation of civil aviation, has asked you to return and lead a review into physical security of airplane cockpits and controls

You have been asked to consider the main lessons should be learned from theses and other relevant incidents and to produce a shortlist of recommendations for actions to be taken to prevent future disasters.

Your review is widely supported including by the both houses of parliament, the public, Airbus, Boeing, Airservices Australia, the major airlines which fly into Australia, the Australian Federation of Air Pilots, the Australian and International Pilots Association, the AFP and ASIO. These parties are all prepared to devote considerable resources to implement your recommendations.

State and justify your top recommendations. Give them in decreasing order of importance (i.e. most important first).

In making your recommendations you have been asked to consider:

- Physical security of Airplane cockpits
- Related policies and practices for air crew on board a flight
- Reevaluate the need for co-pilots to be in the cockpit

- any additional requirements to place on airline companies
- any additional requirements to place on airplane manufacturers
- any additional requirements to place on air traffic controls and on airports
- consider requiring systems to be installed on planes which allow their controls to be overriden by air traffic control towers in extreme events
- Any other such matters relevant to the physical security of the cockpit in oder to prevent the re-occurrence of German Wings type incidents in the future.

Module 5 - Fukushima

Japan split over restart of first nuclear reactor since Fukushima disaster

An otherwise unremarkable town in south-west Japan will be propelled this week to the forefront of the country's biggest experiment with nuclear power since the Fukushima disaster in March 2011.

After months of debate about safety, Japan will begin producing nuclear energy for the first time in almost two years close to the town of Satsumasendai as early as Tuesday.

Restarting one of the Sendai nuclear plant's two 30-year-old reactors represents a victory for the prime minister, Shinzo Abe, who insists that without nuclear energy the Japanese economy will buckle beneath the weight of expensive oil and gas imports.

But his call for Japan to confront its Fukushima demons has been greeted with scepticism by most voters, whose opposition to nuclear restarts remains firm, even in the face of rising electricity bills.

Just over four years since Fukushima Daiichi had a triple meltdown, triggering the world's worst nuclear crisis for 25 years, Japan remains deeply divided over its future energy mix.

The 2011 disaster forced the evacuation of 160,000 people and the closure of all the country's 48 working reactors for safety checks.

Opinions among the 100,000 residents of Satsumasendai range from anxiety to relief.

Local campaigners say the plant operators – Kyushu Electric – and local authorities have yet to explain how they would quickly evacuate tens of thousands of residents in the event of a Fukushima-style meltdown.

"There are schools and hospitals near the plant, but no one has told us how children and the elderly would be evacuated," said Yoshitaka Mukohara, a representative of a group opposing the Sendai restart.

"Naturally there will be gridlock caused by the sheer number of vehicles, landslides, and damaged roads and bridges."

A survey by the Asahi Shimbun newspaper found that only two of 85 medical institutes and 15 of 159 nursing and other care facilities within a 30 km radius of the Sendai plant had proper evacuation plans.

About 220,000 people live within a 30km radius – the size of the Fukushima no-go zone – of the Sendai plant; a 50km radius would draw in Kagoshima city and raise the number of affected people to 900,000. “I can’t begin to imagine how chaotic that would be,” Mukohara said.

Massive earthquakes of the kind that sparked the Fukushima meltdown are not the only potential hazard. The Sendai facility is surrounded by a group of five calderas, and Sakurajima, one of Japan’s most active volcanoes, is just 50km away, leaving the plant exposed to volcanic ash fallout, and, in the most extreme scenario, lava flows.

There are doubts, too, about the reliability of an ageing reactor that has not been used since it was shut down for safety checks in 2011. “You wouldn’t have much faith in a car that’s been on the road for more than 30 years,” said Mukohara. “So why are we so willing to trust a nuclear reactor?”

Shaun Burnie, a nuclear specialist at Greenpeace Germany, accused Japan’s government and nuclear industry of cutting corners in its desperation to put reactors back online.

“They are disregarding fundamental principles of nuclear safety and public health protection,” Burnie said. “The same players in the ‘nuclear village’ that delivered Japan the Fukushima Daiichi tragedy in 2011 are attempting to kick-start nuclear power again.”

Sendai reactor No 1 is one of 25 reactors being targeted for possible restarts. “We’ve finally come this far to restart the first reactor,” the trade and industry minister, Yoichi Miyazawa, told reporters recently. The plant’s second reactor is expected to go back into operation in October.

Last autumn, the Sendai reactors became the first to clear safety hurdles imposed by a revamped nuclear regulation authority. The restart was approved by 19 of the 26 assembly members in Satsumasendai, located 1,000km south-west of Tokyo, and by the pro-nuclear governor of Kagoshima prefecture, Yuichiro Ito.

With national polls showing that most Japanese oppose nuclear restarts, the town’s council is reluctant to gauge local opinion, said Ryoko Torihara, a Satsumasendai resident who is campaigning to the keep the reactors idle.

“They won’t conduct a poll of local people because they’re scared of the result,” she said. “They’re aware that Japan has fared perfectly well without nuclear power for almost two years.”

A nationwide Kyodo News poll last October found that 60% of respondents opposed an immediate return to nuclear energy, while 31% were in favour. But supporters of the restarts say the long hiatus in nuclear energy production has taken its toll on Satsumasendai’s population.

When in operation, the plant contributes up to 3bn yen (£16m) a year to the local economy, according to the local chamber of industry and commerce, much of it via 3,000 workers who descend on the town twice a year to conduct lengthy safety checks.

Satsumasendai continues to receive more than 1bn yen in annual government subsidies for hosting the reactors, but some residents complain keeping the plant shuttered for so long has sucked the life out of local commerce, with hotels, restaurants and other service industries reporting a dramatic drop in trade.

“This is my hometown and I don’t like to see its economy in trouble,” said Tetsuro Setoguchi, a 27-year-old builder. “We receive lots of subsidies for hosting the nuclear plant, and if they dry up it will be difficult for the town to function.

“Lots of jobs depend on the plant, especially in the construction industry. I’m sure that every single builder here wants the reactors to be restarted.”

Kyushu Electric, which last August received a 100bn yen bailout from a state-owned bank to survive, estimates that putting one reactor back online would help it reduce costs from burning fossil fuels by about 7.4bn yen a month. The utility is reeling from four straight years of losses, and nuclear operators across Japan say they have incurred tens of billions of dollars in losses as a result of Fukushima-enforced plant closures.

Before Fukushima, nuclear provided 30% of Japan’s energy needs, and there were plans to increase its share to around 50%. Post-Fukushima, the Abe administration has set nuclear an ambitious target of a 20-22% share of the total energy mix by 2030.

As it prepares to lead Japan into a new, uncertain age of nuclear power generation, the Sendai plant is a fortress protected by high perimeter fences and patrolled by security guards.

At a tent village set up on a windswept beach just along the coast, anti-nuclear activists refuse to accept that Japan’s imminent nuclear reboot is inevitable.

“We will do all we can to stop it,” said Yoshiharu Ogawa, who has travelled from his home near Tokyo. “The local authorities may have approved the restart, but they are completely out of touch with public opinion.”

Japan's post-Fukushima nuclear restart plans dealt a blow by court ruling

A court in Japan has dealt a blow to plans by the prime minister, Shinzo Abe, to relaunch nuclear power generation four years after the Fukushima meltdown by halting the restart of two reactors over safety concerns.

The country's Nuclear Regulation Authority had approved the restart of the reactors at the Takahama plant in Fukui prefecture, but in a ruling on Tuesday judges sided with residents who had sought an injunction against the facility's operator, Kansai Electric Power (Kepco).

The residents had argued that nuclear officials had underestimated the plant's vulnerability to powerful earthquakes of the kind that triggered the Fukushima disaster. They added that the reactors did not meet proper safety standards and that evacuation contingencies were inadequate.

With the nuclear watchdog having approved the restart of the ageing Takahama reactors, as well as two other reactors at the Sendai nuclear power plant in south-western Japan, anxious residents see the courts as their last chance to block the restarts.

The last of Japan's 48 functioning nuclear reactors went offline in September 2013 in response to the March 2011 Fukushima disaster, the world's worst nuclear accident since Chernobyl in 1986.

Another court is to rule this month on a separate injunction brought against plans to restart the Sendai reactors. A similar ruling in that case would in effect derail Abe's campaign to reintroduce nuclear into Japan's energy mix this year. Reports say resolving the legal battles over the four reactors could take months, even years.

The three-judge panel at the Fukui district ruled that the safety of the Takahama reactors had not been secured and described the mooted restarts as "lacking in rationality", according to local media reports.

The presiding judge, Hideaki Higuchi, is considered a maverick in Japan's traditionally conservative judiciary, having issued a similar ruling against separate reactor restarts in Fukui prefecture last May.

Kepco said the residents' injunction was "regrettable and utterly unacceptable" and vowed to appeal against Tuesday's decision.

A lawyer representing the residents hailed a "perfect victory", adding: "This is the best decision we could have expected."

Campaigners said the ruling should prompt a rethink of Japan's energy mix to include a dramatically bigger role for renewables. "This important ruling signals that the government's and the utilities' pro-nuclear agenda can be blocked," said Hisayo Takada of Greenpeace Japan.

"Highly indebted utilities are pushing the restart of their dangerous nuclear plants at any cost – even if their reactors have major safety risks and many are nearing the end of their lifetimes. The decision today is a further setback to a nuclear industry in crisis."

Abe has warned that Japan must restart at least some of its reactors to support the country's economic recovery amid record imports of coal and liquefied natural gas. The business lobby has complained that firms are paying a high price for energy imports while nuclear reactors remain idle.

Kepco, which supplies the sprawling Osaka metropolis, is expecting annual losses of 161bn yen this year and has lost 744bn yen since the Fukushima Daiichi meltdown in March 2011.

Before the ruling, nuclear industry officials had appeared optimistic that reactors would go back online in the coming months.

"This year marks the exit from zero nuclear power," Takashi Imai, chairman of the Japan Atomic Industrial Forum, said at an industry event in Tokyo this week. "It is self-evident that nuclear power plants that have passed safety tests should be restarted as soon as possible."

Japan's pro-nuclear lobby insists that restarts will be critical if Japan is to honour internationally agreed commitments to cut its greenhouse gas emissions.

Environment ministry data released on Tuesday showed that Japan's CO2 emissions rose to the second-highest level on record in the year to March 2014.

Local media reports said Japan aims to reduce CO2 emissions by about 20% from 2005 levels by 2030 – a much lower target than other major developed economies. The post-Fukushima reactor closures had already forced it to slash its previous target to just a 3.8% cut from 2005 levels by 2020.

Before Fukushima, nuclear accounted for almost 30% of Japan's power generation, and there were plans to raise its share even higher with the construction of more reactors.

Despite government pressure to return to nuclear, a majority of the public has been consistent in its opposition restarts since the triple meltdown at Fukushima Daiichi, which sent large quantities of radiation into the air and sea, and forced the evacuation of tens of thousands of residents, many of whom have yet to return home.

Radiation Is Everywhere, but How to Rate Harm?

Since the first reports last month of damage to nuclear reactors at the Fukushima Daiichi power plant, the lingering question has been whether drifting plumes of radioactive elements from the plant will harm people in Japan or other parts of the world. For many people, the biggest fear is cancer.

Certain levels of radiation exposure are known to increase the risk of cancer, but scientists disagree about the effects of very low doses of the sort that may have occurred so far in Japan.

Some researchers say it is reasonable to use data from high doses to calculate the risk of smaller and smaller doses. They argue that any exposure to radiation raises the risk of cancer, though probably by only a small amount in the case of small doses.

But others say that estimating risk for doses near zero is nonsensical, and some believe there is a threshold dose, or limit below which there is no risk from exposure.

Measuring Radioactive Elements and Their Effects APRIL 4, 2011
Dr. John Boice, for example, a professor of medicine at Vanderbilt University who studies radiation effects in humans, warns that risk calculations based on tiny doses are themselves risky.

He argues that there is little data on doses below about 10 rem, but that some risk estimates nonetheless go down to a tenth of a rem or less. (He is also the scientific director of the International Epidemiology Institute in Rockville, Md., a private group that studies radiation with grants from government and industry.)

“I can take a low dose, multiply it by a million people and estimate a risk,” Dr. Boice said, but he said professional groups like the Health Physics Society discourage it. “We say, don’t do that. Don’t multiply a tiny dose by millions and say there will be thousands of deaths. It’s inappropriate, misleading and alarmist. You’ve gone orders of magnitude below where we have proof of any effects at all.”

But Dr. David Brenner, director of the Center for Radiological Research at Columbia University, is among those who believe there is no threshold. Radiation damages DNA, he says, and just one damaged cell can become the seed of a cancer, though it takes decades to develop. He is studying the possibility that in terms of causing cancer, low doses of radiation might be more dangerous than calculations based on high doses would predict.

Current estimates by government agencies for risks from low doses rely on extrapolation from higher doses. In the United States, most government agencies use a unit called the rem to measure radiation doses. (Europe and Asia use the unit millisievert, which equals 0.1 rem.) According to the Environmental Protection Agency, people receive 0.3 rem per year from natural background radiation.

If 10,000 people are each exposed to 1 rem, in small doses over a lifetime (above the natural background exposure), according to the agency, the radiation will cause five or six excess deaths from cancer. In a group that size, about 2,000 would normally die from cancers not caused by radiation, so the extra dose would raise the total to 2,005 or 2,006.

So far only minute amounts of radioactivity from the Japanese reactors have been detected in the United States, in milk on both the East and West Coasts, and in rainfall in Massachusetts. American officials say instruments can detect levels so vanishingly small — far below the natural background level of radiation — that they pose no threat.

In parts of Japan, radioactivity has been detected at various times in milk, meat, vegetables and tap water, on the ground and in the sea around the power plant.

Levels in tap water in certain areas have sometimes been high enough for authorities to tell people to drink bottled water, and the Japanese government has banned the shipment of milk and produce from some prefectures.

Milk from those regions has been found to contain radioactive iodine, which accumulates in the thyroid gland and can cause cancer, especially in children. Levels in the milk have exceeded those considered a cause for concern in the United States.

A quarter mile from the Fukushima plant (residents have been evacuated from a 12-mile zone around the plant) radiation levels of 0.1 rem per hour have been measured, and researchers agree that four days of such exposure would increase a person's risk of cancer. But some would argue that an even shorter exposure would raise the risk.

Many of today's risk estimates are based on a study of 200,000 people who survived the atomic bombing of Hiroshima and Nagasaki in August 1945. More than 40 percent are still alive.

The research has been going on for 63 years, and an article reviewing its findings was published in March in the journal Disaster Medicine and Public Health Preparedness.

So far, it is uncertain how relevant the results from bomb survivors are to members of the public in Japan who may have been exposed to radiation from the reactors.

"One concern is trying to find out what dose these people actually received" from the Fukushima reactors, said Dr. Evan B. Douple, the first author of the article on the bomb survivors and the associate chief of research at the Radiation Effects Research Foundation in Hiroshima, which studies the survivors and is paid for by the governments of Japan and the United States. It is the successor to the Atomic Bomb Casualty Commission, which was created in 1947.

Dr. Douple said the method of exposure was also different: The bomb survivors received their entire doses all at once to the full body, but exposure from the reactors may be gradual.

"Here radioisotopes are drifting in water and air, and not necessarily producing an external whole-body exposure and are being taken up in very small doses into the body," he said. "So far the information we've been receiving is that actually the doses of exposure are not what one would call intermediate or high doses, but are very low."

The bomb survivors received radiation doses ranging from negligible to high; high would be 200 rem or more, what Dr. Douple called a "barely sublethal dose." But 61,000 people were estimated to have received half a rem or less, and 28,000 received half a rem to 10 rem.

Their doses were calculated based on factors like how close they were to the center of the bomb and whether they were inside buildings. For comparison, the study also includes 26,000 people who lived in the same cities but were not exposed to radiation because they were not present during the bombings.

The researchers monitored the two groups — exposed and nonexposed — to determine whether radiation caused disease.

Radiation did increase the risk of cancer. “But the risk of cancer is quite low, lower than what the public might expect,” said Dr. Douple. He said that the researchers themselves had expected to find more cancer than they did.

Among the survivors, leukemia was the first cancer to appear. Cases increased within five years of the bombing and then began declining at the 10-year mark.

Of 120,000 survivors in one study group, 219 with radiation exposure had died of leukemia from 1950 through 2002, the latest year with published data. But only 98 of those cases, or 45 percent, were excess deaths attributed to radiation.

However, when the leukemia deaths were sorted by radiation dose, it was clear that risk increased with dose. Among people who received the highest doses (100 rem or more), 86 percent of the leukemia deaths were a result of radiation, compared with only 36 percent of the leukemia deaths in those with exposures from 10 rem to 50 rem. Among those who received half a rem to 10 rem, only 4 of 77 leukemia deaths, or 5 percent, were estimated to be excess deaths caused by radiation.

Solid tumors — affecting the colon, breast, liver, lung or other organs — took longer than leukemia to develop, Dr. Douple said.

In a study group of 100,000, there were 7,851 deaths from solid cancers among people exposed to radiation, but only 850, or 11 percent, were estimated to be excess cancer deaths due to radiation. As with leukemia, the risk increased with radiation dose. Some organs were more sensitive than others. For instance, radiation increased cancer risk in the breast, but not the prostate.

Dr. Douple emphasized that at very low doses, the risk was also very low. But he also said that there was no indication of a threshold, or a level below which acute radiation exposure would have no effect, or a smaller effect than would be predicted based on higher exposures.

Does the bomb data apply to Fukushima? Hiroshima and Nagasaki were the worst case, Dr. Douple said. It is possible to extrapolate from them to the very low-dose range detected so far, but in doing so, he said, there are “big uncertainties.”

But he added that Japanese scientists from the institute have been summoned to Tokyo, to help figure out what the potential health effects might be and to plan ways to detect and study them.

Is your fear of radiation irrational?

Bad Gastein in the Austrian Alps. It's 10am on a Wednesday in early March, cold and snowy – but not in the entrance to the main gallery of what was once a gold mine. Togged out in swimming trunks, flip-flops and a bath robe, I have just squeezed into one of the carriages of a narrow-gauge railway that's about to carry me 2 km into the heart of the Radhausberg mountain.

Fifteen minutes later we're there and I'm ready to enjoy what the brochures insist will be a health-enhancing environment. Enjoyment, of course, is a subjective term. The temperature inside the mountain's dimly lit tunnels is around 40°C, and the humidity is 100 per cent. The sweat's already begun to flow. More important, I'm breathing an atmosphere rich in radon.

Hang on… radon? That's a radioactive gas. Yet here I am, without so much as a film badge dosimeter, never mind the protection of a lead apron, among a group of people who have paid to come to the Gasteiner Heilstollen ("healing galleries") and willingly, even eagerly, undergo gruelling sessions in physical discomfort because of a much-contested theory that small doses of radiation are not just harmless, but act as a stimulant to good health.

Our view of radiation and its risks and benefits is complicated and mostly – the delights of the Heilstollen notwithstanding – negative. We are all aware of the effects of a nuclear weapon, the Armageddon scenario of a nuclear winter, cancers and birth defects caused by high doses of radiation and the like. Images of mushroom clouds have struck fear into our hearts since the 1940s, but it is what we can't see in those pictures that scares us the most.

Invisible threats are always the most unnerving, and radiation is not something you can see. Nor can you control it. Many years ago, a veteran researcher told me how much he wished he could paint radiation blue. If we could see it, he said, we'd be better placed to deal with it and less nervous about it. The traditional secrecy of the biggest commercial user of radiation, the nuclear power industry, hasn't helped. Only belatedly did it realise that doing things out of sight, behind closed doors, is the best way to fuel public suspicion. So it is perhaps understandable why many people say that (medical X-rays and CT scans aside) the only safe radiation is no radiation.

Nevertheless, I disagree. I believe that a justified fear of high and uncontrolled levels of radiation has undermined our willingness to see that the risks it poses at low levels are either acceptable or manageable. Imagine if we treated fire in the same way as all things nuclear: we would have responded to house fires by banning matches.

And I am worried that, as a result of these exaggerated fears, we are failing to make the most of radiation for our greater good.

To appreciate the measure of our hot-button fixation with radioactivity, recall the events of 2011 in Japan. The magnitude 9 earthquake and subsequent tsunami that hit the country on 11 March was by any measure a disaster. 20,000 people died and more than 500 square kilometres of land were flooded. Families lost their homes, their businesses and their livelihoods.

It didn't take long for the media to discover that one of the casualties, in pole position when the tsunami struck, was the Fukushima nuclear power station. From that moment the story ceased to be about a natural event and became, in effect, about a man-made one. It became that chilling scenario: a nuclear disaster.

Of the 20,000 deaths, some were directly due to the earthquake itself, while others were caused by drowning. How many deaths were the result of radiation from the damaged plant? None. In its section on the health consequences of the Fukushima tragedy, the report by the UN's Scientific Committee on the Effects of Atomic Radiation says: "No radiation-related deaths or acute diseases have been observed among the workers and general public exposed to radiation from the accident."

The dose to the public, the report goes on to say, was generally low or very low. "No discernible increased incidence of radiation-related health effects are expected among exposed members of the public or their descendants."

This is not to play down the impact of the event. Three of the nuclear plant's reactors suffered damage to their cores, and a large amount of radioactive material was released into the environment. Twelve workers are thought to have received doses of iodine-131 that will increase their risk of developing cancer of the thyroid gland. A further 160 workers experienced doses sufficient to increase their risk of other cancers. "However," says the report, "any increased incidence of cancer in this group is expected to be indiscernible because of the difficulty of confirming such a small incidence against the normal statistical fluctuations in cancer incidence."

In short, while a terrifying natural event had killed many thousands of people, the focus of attention in Japan and round the world was on one component of the tragedy that killed no one at the time. Radiation exposure may have shortened the lives of some of those directly involved, but its effects are likely to be so small that we may never know for sure whether they are related to the accident or not.

When it comes to disaster, nuclear trumps natural. Our sense of the relative importance of things is absurdly skewed.

§

Chernobyl, of course, was much worse. A poorly designed reactor operating under weak safety arrangements in a bureaucratic and secretive society was a recipe for disaster. On 26 April 1986 all the ingredients came together – ironically during an experimental and bungled

safety check. One of the reactors overheated, caught fire, exploded and released a large quantity of radioactive material into the atmosphere. 116,000 people were evacuated; another 270,000 found themselves living in a zone described as “highly contaminated”.

It sounds bad. For 134 of the workers involved in the initial cleanup, it was very bad. The dose they received was enough to cause acute radiation sickness, and 28 of them soon died. Then, distrust of official information together with rumours of the dire consequences to be expected created a disproportionate fear. One rumour circulating during the period immediately following the accident claimed that 15,000 nuclear victims had been buried in a mass grave. Nor did such rumours die away; another in 2000 held that 300,000 people had by that time died of radiation.

The reality, though hardly inconsequential, was less catastrophic. A World Health Organization expert group was set up to examine the aftermath of the disaster and to calculate its future health consequences. On the basis of average radiation exposure for the evacuees, the people who weren’t evacuated and the many more thousands of workers later involved in the cleanup, the report concluded that cancer deaths in these three groups will increase by no more than 4 per cent. The report’s conclusions have been, and still are, contested – but the weight of orthodox opinion continues to line up behind the expert group’s calculations.

“There was certainly a rise in thyroid cancer,” says James Smith, Professor of Environmental Science at Portsmouth University and a coordinator of three multinational European Community projects on the environmental consequences of the accident. But he goes on to add a qualification: “The Soviets didn’t put in enough measures to stop people eating contaminated food and drinking contaminated milk, and this particularly affected children.” The deaths, in other words, were not all inevitable.

Any death from any cause in any industry is regrettable and, ideally, to be prevented. But is nuclear power inherently more dangerous than other forms of energy? A 2002 review issued by the International Energy Agency compared fatalities per unit of power produced from several energy sources, including coal, biomass, wind and nuclear. The figures included each stage of energy generation from the extraction of any raw materials required to the health consequences of generating and using it.

Coal came out on top while nuclear emerged as the least damaging to health. When you think of coal-fired energy generation, from the hazards of mining to atmospheric pollution, this rank order is hardly surprising. But while the choking murk over many big Asian cities on a still day is clear to see, deaths related to the coal industry don’t mobilise either fear or indignation on the same scale as a nuclear incident does. Perhaps it is radiation’s invisibility that fuels overheated reporting of relatively minor events – and then the reporting, by its extent as much as by sensationalism, confirms and heightens our fear.

§

A number of governments responded to the events in Japan in 2011. Most notable was Germany. Although unenthusiastic about nuclear power, it had recently accepted a need to

prolong the period for which its existing nuclear plants would operate. Following the events at Fukushima, it changed its mind. Critics of the policy change were left trying to recall the last time Germany had experienced a really severe earthquake, never mind a tsunami.

Ironically, despite being a nation encompassing some of Europe's most strident opponents of nuclear power, Germans make up a significant proportion of visitors to the radon-rich clinic at Bad Gastein.

The particular Gasteiner Heilstollen tunnel in which I spent my 30 radon-breathing minutes had room for 20 or so people who had signed on for its protective value or its alleged benefit in alleviating conditions such as rheumatoid arthritis, asthma and sinusitis or skin conditions like psoriasis.

The doctor in charge on the day of my visit was Simon Gütl. He told me of clinical trials, of surveys testifying to the popularity of the treatment, and of patients who are able to cut down on or even abandon the drug therapies they would otherwise have been using. How much of this evidence would rate as gold standard in quality, I have no idea – but I was struck by the enthusiasm with which some people seek out the same force of nature that most others think we have to avoid at any cost. One of my fellow transient troglodytes was on her 70th visit.

The managing director of the Gasteiner Heilstollen is Christoph Köstinger, a physicist by education. Some 9,000 patients, he told me, do a full spa therapy of one session per day for 2–4 weeks, and several thousand more have shorter courses. He is well aware of people's conflicting feelings about radiation: "I divide people into three groups," he says. "Those who are really frightened of radiation don't come to us. Then there are people who are not frightened of radiation and say it's all OK. And a lot of people are a little bit frightened, but you can usually explain the balance of risk."

He's also aware of the widespread aversion to nuclear power throughout Germany. "Some patients explain it to themselves by saying that this [radon] is natural radiation," he explains, hastening to add that as a physicist he's aware of the meaninglessness of any distinction between 'natural' and 'unnatural' radiation.

§

Lying on my bed of discomfort in the Gastein galleries, breathing in the radon, just how much radioactivity was I taking on board? Very little. I was inside the mine for slightly over an hour. Köstinger reckons that during a three-week treatment programme, patients receive a dose of around 1.8 mSv (millisieverts), or roughly three-quarters of a full year's background radiation – because, of course, we are all exposed to low-level radiation all the time.

First, there is cosmic radiation from the Sun and the rest of the stars in our galaxy and beyond. How much we get depends on the altitude at which we live and on fluctuations in the Earth's magnetic field. And then there's radiation from the Earth itself, including radon. Here, too, geography is a factor: in some places radon can be found leaking into the atmosphere in significantly larger amounts. Naturally radioactive solids such as uranium and

thorium in rock and soil also make their contribution. The global average annual radiation dose is 2.4 mSv. To put this in perspective, that's about the same as 120 chest X-rays.

Much of what we know about radiation's effects on human beings comes from far higher doses following nuclear explosions – the bombs dropped in 1945 on Hiroshima and Nagasaki. The Radiation Effects Research Foundation has studied the health of some 100,000 survivors of the two bombings, and the health of their children.

The findings from the survivors themselves came as no great surprise. For cancers other than leukaemia, an excess risk started to appear about ten years after the event. The extent of the risk depended on each individual's distance from the site of the explosion, as well as on age and gender. As an example, anyone about 2.5 km away had a 10 per cent greater risk of developing a tumour. In the case of leukaemia, the excess number of deaths began to appear just two years after exposure and peaked four to six years later.

What hadn't been expected were the findings from the Hiroshima and Nagasaki survivors' children. The assumption had been that they too would be more likely to develop malignancies of some kind – but so far this has not been the case.

"At this point we have not seen any excess of cancer or non-cancer mortality," says Roy Shore, chief of research at the Radiation Effects Research Foundation. He goes on to point out that a large part of their disease experience will occur over the next 30 years, so he can't entirely rule out a late effect. Nonetheless, the findings so far are a bit of a surprise. "Based on experimental data ranging from fruit flies to mice we would have expected to see some," he adds.

§

Of the unresolved debates about radiation, the most contentious is the true extent of the harm (or even the benefit, if the Gasteiner Heilstollen evidence persuades you) that it causes at low levels.

There are two schools of thought. The generally accepted view derives from the known relationship between higher levels of radiation exposure and the subsequent likelihood of developing cancer. Plot one against the other, and what emerges is a more-or-less straight line. The uncertainty is over this being extrapolated to very low doses, and whether there is a threshold below which the risk vanishes.

"At really low doses – down in the range of, say, a CT examination – we don't have strong evidence one way or another," says Shore. "It's a matter of interpretation." He himself sees it as prudent to assume there isn't a threshold: the so-called 'linear no-threshold' (LNT) hypothesis.

Professor Gerry Thomas has a chair in molecular pathology at Imperial College London and takes a close interest in the effects of radiation. As she points out, illnesses caused by radiation are also caused by other things, so at the lower end of the dose range you need a

very large group of people to prove it either way. “Most scientific opinion is that there’s no data to say it’s dangerous until you reach about 100 mSv.”

Even so, most radiation regulatory authorities and their advisers back the LNT view. Safety limits are set accordingly low. The upper limit for exposure for a member of the UK public, for example, is 1 mSv per year – less than half the annual average background dose.

Speaking for the Bad Gastein clinic, Köstinger takes a pragmatic view. He balances the risk of low-dose radiation against what he describes as the “scientifically proven effect” of the treatment. “We have a hypothetical risk [from radiation],” he says, “but even in the worst case it is minimal compared to the risks of the drugs our patients are usually able to stop using. If there’s a risk, we can live with it. If scientific knowledge suggests there’s a threshold, that’s also OK.”

The overall conclusion of all this is that radiation is nothing like as damaging as is commonly assumed. Moreover, what often gets lost in the argument is that the difference between a very small risk and a slightly greater very small risk may be of no practical consequence. In fact, policies and decisions that become obsessed with radiation risk minimisation may, in the wider scheme of things, turn out to be counterproductive.

§

Does it matter if large numbers of people have an unwarranted dread of radiation? After all, millions of us have irrational fears about all sorts of things from spiders to flying. We cope. The world still turns.

Two instances serve to illustrate why being unduly fearful of radiation does matter. Both, in their way, are troublesome for individuals and for the community.

The first is our reluctance to exploit nuclear power. From 1970 onward, global electricity production from nuclear power stations experienced a steady rise. In the 1990s, this rise continued, but at a slower pace. From 2000, it flattened out, and then began to slip. Even as enthusiasm for carbon-free energy generation began to increase, the use of carbon-free nuclear power first faltered, then began to decline.

There are many reasons for this, not least the arguments about the cost of building nuclear power stations and of decommissioning them. But public suspicion has possibly – probably – had the key role in policy decisions. We’ve watched as nuclear power stations have begun to reach the end of their working lives. In panic at the prospect of the lights going off, we’ve extended those lives. But some countries have shied away from replacing them, judging that the perceived risk is greater than the potential role of nuclear power to significantly limit man-made climate change. From the evidence, it seems clear to me that the balance lies overwhelmingly in the other direction.

The personal consequences of an excessive fear of radiation are, in their way, even more damaging. Evidence for this can be found in the aftermath of the events at Chernobyl and

Fukushima. The WHO Expert Group set up to examine the Chernobyl disaster reported that it had a serious impact on the mental health and wellbeing of the local population who were evacuated.

“There are sad stories from Chernobyl and more recently at Fukushima of people being shunned by the communities they went to because they were thought to be radioactive or in some way contaminated,” says Smith. “One conclusion of the WHO report was that the social and psychological impacts of Chernobyl had been worse than the direct radiation impacts.”

He recalls meeting a man fishing in a contaminated lake within the Chernobyl exclusion zone. “This guy said he wasn’t moving: ‘The Second World War didn’t move me out of my home, so I’m not going to go on account of a bit of radiation.’

“You can’t say for sure, because it’s all about statistics, but he probably made the right decision. He certainly faced an additional risk because he was eating local food, which was contaminated, but the risk he would have taken on if he’d been forced to move to somewhere else and live a different lifestyle would probably have meant he lived less long anyway.”

Although the Fukushima evacuees were less plagued by outlandish rumours than their counterparts at Chernobyl, they too suffered the nagging consequences of an undue fear of radiation and its unpredictable effects on health. A 2012 survey of the evacuees revealed that one in five of them showed signs of mental trauma.

Stress and consequent mental health problems are unavoidable when evacuation and relocation is indisputably necessary. But a zealous application of the precautionary principle, worst-case assumptions about the effects of radiation and wide safety margins have fostered counterproductive risk assessments. Together with unfounded rumour, sometimes boosted by secrecy on the part of officialdom and a reluctance to confront irrational suspicions, radiation has become everyone’s worst nightmare.

§

Rumbling through the train tunnel on the way out of the Gasteiner Heilstollen, I remembered the idea about painting radiation blue. Whimsically, seeking distraction from the humid heat, I wondered what it would be like if we were consciously aware of radiation. Not by painting it, but by some other means.

Imagine if our eyes could see far beyond the visible region of the spectrum and act as a radiation detector, able to signal everything to the brain as a visual sensation – or even as an auditory one. Or if our skin evolved to tingle in the presence of radiation. But radiation is everywhere, and ever-present. If we could sense it, it would be too distracting, all the time.

One man-made alternative is obvious: imagine cheap and universally available wristwatch-sized Geiger counters set to stay silent – crucial, this – below radiation levels with epidemiologically discernible consequences. Wearers predisposed to being nervous about

radiation might be surprised never to hear their detector going off. Certainly not during my trip under the mountain. Not during a whole-body CT scan. Not even during a week's camping holiday beside the cemetery at Chernobyl.

But would that be enough to reassure you?

Question

You are the head of the Japanese Nuclear Regulation Authority (NRA) 原子力規制委員会 and have been asked to reconsider the NRA's approval of restarting Japan's Nuclear reactors (shutdown after the 2011 Tsunami). There is considerable opposition from local residents concerned about the risks of radiation to themselves and their families if there were to be another catastrophe. The private operator of the plant has stated that they have learned form the IAEA report into the accident and can be trusted to redesign and operate the plant with appropriate safely in the future.

Prime minister Shinzo Abe is finding it hard to assess the competing claims and assurances of proponents and opponents to the plant's re-opening, and has asked you, an expert he trusts, to give him a very brief briefing about what he should do. He has asked you to consider the risks arising from potential future catastrophes, human errors, and other unforeseen or out of ordinary events and to rule on whether it is feasible and reasonable to restart the country's reactors.
Your ruling may be YES, NO, or CONDITIONAL.
If you rule CONDITIONAL then you are to recommend reasonable conditions which need to be met in order for the approval to be granted.
Give the main reasons for your ruling, including factors favouring the other ruling which you considered but were not sufficient to change your ruling.
Make your reasoning clear and compelling and even handed. A reasonable person reading your decision and reasoning should not feel you were biased or had made your mind up in advance. However your ruling needs to be clearly supported by your reasoning - for example it would not be good to rule YES and then list a long list of arguments each way and leave the reader to make the opposite decision.
Abe calls you into his office and explains, unofficially, that he will not be happy if you conditionally approve and then impose a list of impractical conditions as a easily way of getting out of saying NO. Your YES should mean YES, your NO should mean no, and CONDITIONAL approval must mean it is genuinely possible to proceed subject to a feasible amount of work and expense.
Write your report as a private blog post private subpage of your profile page* (private to you and your tutor) state your RULING, give your reasoning, and any (reasonably achievable) conditions you impose. Limit 250 words.
Bring a printout of your report to the tutorial. After the end of the week make your blog post visible to everyone.

Module 7 - Johnny Cab

Introduction

Land (aka Real Property) is most people's main asset, and is incredibly valuable. It has special laws to protect and regulate sale and ownership.

Once you buy it in good faith and the sake is "registered" in many places in the world this means the sale is a done deal and there is no going back - sometimes even if the real owner didn't sell it the new owner can own it. Wow...

NSW is considering selling the land titles office (called the LPI) (stop-press: the sale aka a 35 year lease just went thru last week - But let's rewind the clock and suppose it has not yet been sold) Should it be?

Research real property assets and law and history of crime and scams and cons. Research the sale of the LPI and the pros and cons. Heck you can even visit the LPI in the city and check it out.

Question

1. What are the cyber related risks of sale of the LPI?
2. What are the cyber risks faced by the LPI?
3. In general, what are cyber risks facing landowners - including but not limited to the LPI sale?
4. If someone you loved was buying or selling property how would you advise them with respect to security?

Module 10 - Reagan

Attempted assassination of Ronald Reagan (Intro)

On March 30, 1981, a shooting occurred at the Washington Hilton Hotel in Washington D.C., which targeted Ronald Reagan, the 40th President of the United States. While leaving a speaking engagement at the Washington Hilton Hotel in Washington, D.C., President Reagan and three others were shot and wounded by John Hinckley Jr.. Hinckley's motivation for the attack was to impress actress Jodie Foster, over whom he had developed an obsession after seeing her in the 1976 film Taxi Driver.

There were no fatalities in the immediate aftermath of the attack. Reagan was shot in the chest, just below the left underarm. He suffered a punctured lung and heavy internal bleeding, but prompt medical attention allowed him to recover quickly. No formal invocation of presidential succession took place, although Secretary of State Alexander Haig controversially stated that he was "in control here" while Vice President George H. W. Bush returned to Washington.

The most seriously wounded victim was White House Press Secretary James Brady, who was left paralyzed from a gunshot wound to the head. He would later die in 2014 of causes a Virginia medical examiner found were directly related to the 1981 shooting.[1][2] Hinckley also wounded Secret Service agent Tim McCarthy and Washington D.C. police officer Thomas Delahanty.

Hinckley was found not guilty by reason of insanity on charges of attempting to assassinate the President at his trial, and Foster was required by a federal judge to testify. Hinckley remained confined to a psychiatric facility. On July 27, 2016 it was announced he would be released to live with his mother in Williamsburg, Virginia, no earlier than August 5; he was subsequently released on September 10.[3] In January 2015, federal prosecutors announced that they would not charge Hinckley with Brady's death, despite the medical examiner's classification of his death as a homicide.[4]

Columbine High School massacre (Intro)

The Columbine High School massacre was a school shooting that occurred on April 20, 1999, at Columbine High School in Columbine,[3][4] an unincorporated area of Jefferson County in the American state of Colorado. In addition to the shootings, the complex and highly planned attack involved a fire bomb to divert firefighters, propane tanks converted to bombs placed in the cafeteria, 99 explosive devices, and carbombs. The perpetrators, senior students Eric Harris and Dylan Klebold, murdered 12 students and one teacher. They injured 21 additional people, and three more were injured while attempting to escape the school. The pair subsequently committed suicide.[5][6]

Although their precise motives remain unclear, the personal journals of the perpetrators document that they wished their actions to rival the Oklahoma City bombing and other deadly incidents in the United States in the 1990s. The attack has been referred to by USA Today as a "suicidal attack [that was] planned as a grand—if badly implemented—terrorist bombing."[7] The massacre has been reported as "the deadliest high school shooting in US history."[8]

The massacre sparked debate over gun control laws, high school cliques, subcultures, and bullying. It resulted in an increased emphasis on school security with zero tolerance policies,[9][10] and a moral panic over goth culture, gun culture, social outcasts (even though the perpetrators were not outcasts),[11][12] the use of pharmaceutical anti-depressants by teenagers, teenage Internet use,[13] and violence in video games.[14][15]

Question

- Last week was the anniversary of the Kent State Massacre - the May 4, 1970 killing of unarmed college students protesting the Vietnam War at Kent State University by members of the Ohio National Guard. It is an appropriate time to consider incident response.
- Gun violence in the US is not like anything we are used to here. 17 of their presidents have had assassination attempts.
- Consider the assassination of Reagun for example.
- (Discuss in your blog your thoughts on the president's security planning and the way the indecent is responded to by all those involved)
- Similarly the US has an appalling history of gun violence at schools.
- The Secret Service wrote a report analysing such incidents.
- The scenario question this week will be about preparing for and responding to such incidents. Read around the above incidents so you know the background of the cases and likely contributing factors, and think about planning and good and bad responses.

Module 11 - Disaster

Disasters are regular occurrences - you don't know know where (with the exception of the San Andreas fault) or when they will strike, but you know that they will strike. We have lots of data about past natural disasters - we can learn from that in planning for and responding to cyber disasters.

This week's scenario is about responding to and planning for disaster. We'll give you a scenario and ask you how you would respond in it as an individual. We'll also ask you to travel back in time to a year before the disaster (when it was not specifically anticipated) and ask what you should do to prepare for it - as the prime minister or head of some government disaster planning body.

Read about the following disasters, how most people died, what went right and what went wrong in the immediate response.

Hurricane Katrina
The Great Chicago Fire of 1871
The 2004 Boxing Day Tsunami
This Tsunami had more energy than all the explosives detonated in WWII including the two atom bombs.

Despite taking several hours to reach the more distant places it struck, most people were taken completely unaware.

see a time log :
http://www.telegraph.co.uk/news/worldnews/asia/indonesia/11309215/How-the-Boxing-Day-tsunami-unfolded-hour-by-hour.html

From wikipedia:

One of the few coastal areas to evacuate ahead of the tsunami was on the Indonesian island of Simeulue, very close to the epicentre. Island folklore recounted an earthquake and tsunami in 1907, and the islanders fled to inland hills after the initial shaking and before the tsunami struck. These tales and oral folklore from previous generations may have helped the survival of the inhabitants.[54] On Maikhao beach in northern Phuket, Thailand, a 10-year-old British tourist named Tilly Smith had studied tsunami in geography at school and recognised the warning signs of the receding ocean and frothing bubbles. She and her parents warned others on the beach, which was evacuated safely.[55] John Chroston, a biology teacher from Scotland, also recognised the signs at Kamala Bay north of Phuket, taking a busload of vacationers and locals to safety on higher ground.

Anthropologists had initially expected the aboriginal population of the Andaman Islands to be badly affected by the tsunami and even feared the already depopulated Onge tribe could have been wiped out.[56] Many of the aboriginal tribes evacuated and suffered fewer casualties.[57][58] Oral traditions developed from previous earthquakes helped the aboriginal tribes escape the tsunami. For example, the folklore of the Onges talks of "huge shaking of ground followed by high wall of water". Almost all of the Onge people seemed to have survived the tsunami.[59]

How the Boxing Day tsunami unfolded, hour by hour

On December 26, 2004, the western coast of Indonesia was shaken by a 9.2 magnitude earthquake, the fourth biggest in recent times. The damage was felt in 14 countries, and 1.7m were made homeless in the aftermath.
But at first, the huge scale of the quake and subsequent tsunamis wasn't immediately clear. Explore the graphic above (or click here for the whole page experience) to see what happened in the hours after the Indonesian quake, as the ripples spread throughout Asia and the world woke up to one of the most devastating natural disasters ever.
00:59 GMT
The third largest earthquake ever recorded strikes off the west coast of Sumatra, Indonesia. With a magnitude of between 9.1 and 9.3, it unleashes a force 1,500 times greater than the atomic bomb that levelled Hiroshima and rips an 800-mile-long gash in the sea bed.
It is also the longest earthquake ever recorded, lasting for between eight and ten minutes. Normally, a moderate earthquake might last a few seconds.
15 minutes in

The first warning comes from the Pacific Tsunami Warning Centre in Hawaii, which issues a bulletin that an earthquake has taken place. But there is initial confusion over the strength of the quake. In Indonesia, the authorities say it is 6.6 magnitude while geologists in the United States say it was 8.1.

There was no tsunami warning system in the Indian Ocean to detect tsunamis or to warn the hundreds of thousands of people who lived in coastal areas.

30 minutes

A tsunami hits the northern tip of Indonesia, just 65 miles from the epicentre, devastating the coast and eventually claiming more than 130,000 lives. More than half a million people lost their homes. Banda Aceh is the worst hit, with more than 60 per cent of its buildings destroyed by a wave that was over 30ft high.

35 minutes

The Nicobar and Andaman Islands are hit next, with an estimated 1,894 dead. The indigenous tribes living on the island had move to higher ground after the quake and escaped disaster.

1 hour

The wave arrives in Burma, where 59 eventually died, and in Malaysia, killing 89. Even at this point, there is no official confirmation of a tsunami and the number of victims is assumed to be just nine.

Despite a long lag between the time of the earthquake and the arrival of the tsunami, almost all the victims are taken completely by surprise.

1 hour 30 minutes

Reports start to arrive that the west coast of Thailand and Phuket have been hit by a huge wave. Tourists watched as water recedes from the beach before washing back over them. Eventually, more than 5,300 people on the Thai coast would lose their lives. Many tourists drowned in their hotel rooms. The US upgrades the strength of the quake to 8.9 magnitude.

2 hours

Seismologists record another earthquake, of 7.3 magnitude, near the Andaman and Nicobar Islands. At the same time, the wave hits Sri Lanka and southern India, destroying fishing villages and coastal towns. As many as 31,000 people die on the east of Sri Lanka. Satellites record tsunami wave heights over the Bay of Bengal, but data doesn't reach scientists until hours later.

2 hours, 30 mins

At least 8,800 people are killed on the south east coast of India around Chennai, but statistics are slow to come in. In India and Sri Lanka many of the victims are women and children: the men who were out fishing floated over the wave, only to return to towns and villages that have been utterly destroyed.

News of mass casualties in Sri Lanka starts to trickle out, but statistics still under represent the scale of the disasters.

3 hours, 30 mins

The wave washes over the low-lying Maldives islands, claiming 82 lives.

7 hours, 15 mins

In an indication of the scale of the tsunami, the wave reaches the east coast of Africa, some 4,400 miles away. Somalia is the worst affected area, with 150 deaths, but the wave destroys homes and poisons water supplies.

14 hours, 30 mins

Waves from tsunami reach the Pacific and the water mark in Mexico rises by 8ft. Over the coming days, as the scale of the emergency becomes clear, a series of aftershocks hamper what will become the world’s largest-ever relief operation.

Question

Suppose one of the following has happened (consider each in turn):

Earthquake

You are at uni, it is today. You feel an obvious tremor for about 5 minutes. Everyone evacuates the buildings.

The internet says there has been an unprecedented and giant earthquake far off the coast of New South Sales. All over the Internet people are joking about the possibility of a Tsunami. News channels say "events unfolding" and "more information as it coms to hand". A network traffic reporter on a helicopter reports some small fires in the CBD, traffic chaos, and unconfirmed reports of some damages to bridges.

For each of the below consider and rank alternatives as well as deciding which is your top ranked course of action - and give reasons:

a) Pretend you are yourself - what do you do ?
b) Pretend you are the uni - what do you do?
c) Pretend you are the government minister for emergencies - what do you do?

For each of the above discuss what you should have done BEFORE today to be prepared for this.

Tropical Cyclone

Tropical Cyclone Donald is moving remarkably far south. It is making erratic movements but you hear on the radio that experts now think there is a reasonable chance it might make landfall in or near Sydney sometime within the next 24 hours. It is currently a category 5 cyclone, which is the most extreme, and moving rapidly.

You woke this morning to hear about this on the radio. It is a uni day. What do you do?
a) Pretend you are yourself - what do you do ?
b) Pretend you are the uni - what do you do?
c) Pretend you are the government minister for emergencies - what do you do?

For each of the above discuss what you should have done BEFORE today to be prepared for this.

Extended Presentations

Lock Picking

- The typical lock is made up of several pins, that are held in cylinders and .
- The pins are of varying heights and will therefore block the rotation of the lock in the state where no key is present or an incorrect key is inserted.
- When the correct key is inserted, it raises the pins to just the right height so the lock can rotate.
- However, due to inconsistencies in the production of locks, the pins are usually of different sizes or are not aligned properly, which makes it so that a slight rotation in the tumbler will make a set pin stay in position.
- To break this type of lock (pin tumbler locks), a pick is used to lift the individual pins, whilst a tension wrench applies pressure so that once any binded pins stay in position. Once all the pins are pushed to the right position (shear line), the lock will then turn and is considered to be picked.
- Another technique is raking. This works by using a special type of pick that moves in and out of the lock quickly to try and push the pins into the right position by chance.
- Other ways to open locks include:
    - Bump keys - A key that is hammered into the lock and bumps the top cylinders up and allow for rotation.
    - Snap guns - work in a similar way to bump keys, tapping the bottom cylinders and causing the top cylinder to jump up.
- Moral of story - Most locks are poor physical security and easy to break given the right tools and techniques

Smashing the Stack

- Canaries Canaries are known values that are placed between a buffer and a control data on the stack to monitor buffer overflows. When a buffer overflows the first data to be corrupted will be the Canary and a trigger will occur. Canary's are a great way to pad or protect a program from invalid memory access.
- Sentinel value, also known as a flag value, trip value, rogue value, signal value, dummy data, it is used to show out of bands and prevent overflows. AKA like a flag that trips and ends the process
- Terminator canaries use the observation that most buffer overflow attacks are based on certain string operations which end at string terminators.
- Random Canaries Random canaries are randomly generated, in order to prevent an attacker from knowing their value. Usually, it is not logically possible or plausible to read the canary for exploiting; the canary is a secure value known only by those who need to know it—the buffer overflow protection code in this case.

- XOR canaries Random XOR canaries are random canaries that are XOR-scrambled using all or part of the control data. In this way, once the canary or the control data is clobbered, the canary value is wrong.
- **Canaries**, which act as a tamper seal
- **ASLR** - which randomise the memory every time so you can't predict certain addresses.
- **NX** - Which makes the stack non-executable (read only)
- **PIE** - A position independent executable, which can run regardless of the positions of all of its code
- **Shadow Stacks** - Where it doesn't matter if you can change the stack, as you read from a shadow stack instead which stores all the return addresses separate from the writeable memory.

OpSec

VPNs

Vpns work by encrypting a packet that is sent to the VPN, which the VPN then sends out to the world as a proxy for you. That data is then sent back to the VPN and encrypted again when the packets are sent back to you. This prevents ISP's from eavesdropping on you.

TOR

The TOR Onion comes from the multiple layers of security per router, and you never know if it’s from the router or from the source. Everyone knows who came before but no one knows the start and end.

However, there are still exit node vulnerabilities that you should be aware of.

Format Strings

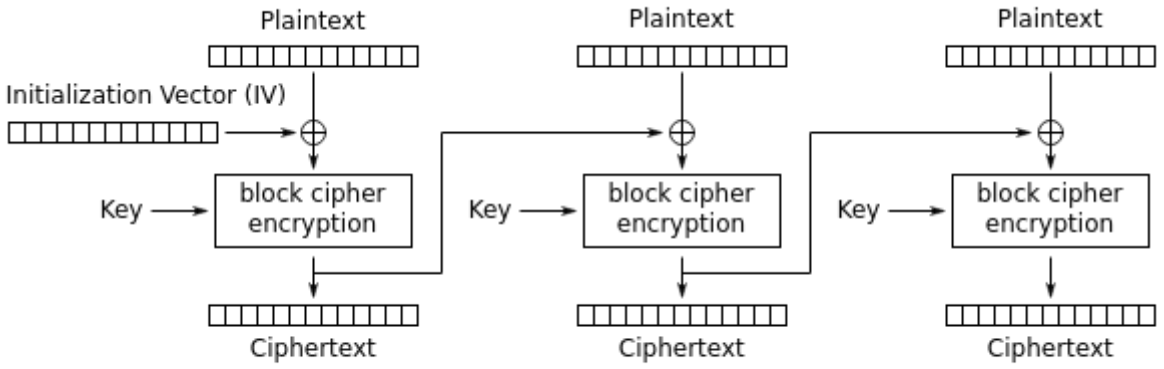
- C parses format strings by the memory location of its arguments, which means that once you have access to a format string, you can easily tell C from what memory address to print from by just specifying where on the stack you variable is.
- Through this you can use things like %s or %x to just print from the stack as you wish, which means you can look around and print variables that you shouldn’t have access to.
- You can even use things like %n to write to memory the number of bytes you’ve currently written.
- These vulnerabilities happen when we have both the control and user data in the same outlet.
    - For example, when we have `printf(“%s”, str)`

- We explicitly separate the user data and the control data, telling C to print the variable str as a string.
- However, if we were to do something like this `printf(str)`
- Then C will just read the str buffer as a control sequence as well, meaning the user can enter in and use control data such as %s and %x however they like.

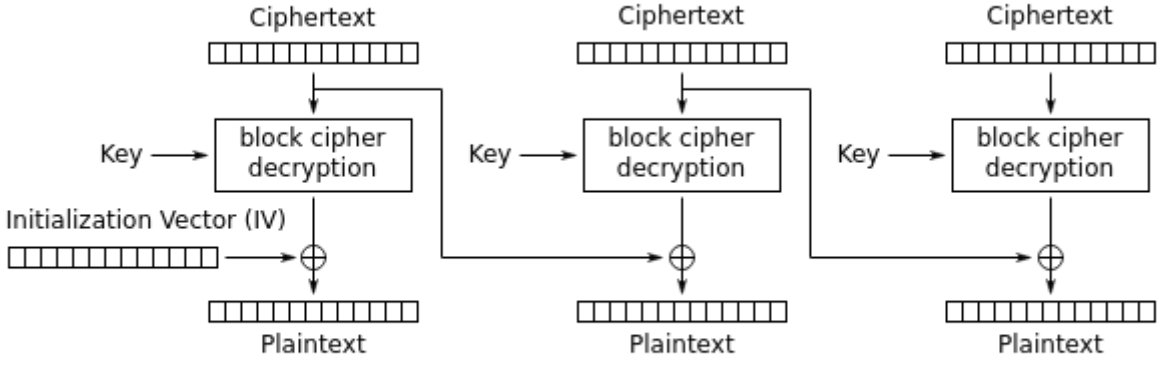
Padding Oracle Attack (PKCS7)

Chain Block Cipher (CBC)

- Chain block ciphers is an encryption algorithm which encodes a message by fixed sized blocks. Each block is encrypted by xoring the previous ciphertext block to the plain text, and passing the result of the xor through a encoding scheme e.g. AES. Since the first block does not have a previous ciphertext block to xor it with, it is xored with an initial vector (IV) instead.



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

If the first block has index 1, the mathematical formula for CBC encryption is:

$$C_i = E_K(P_i \oplus C_{i-1}),$$

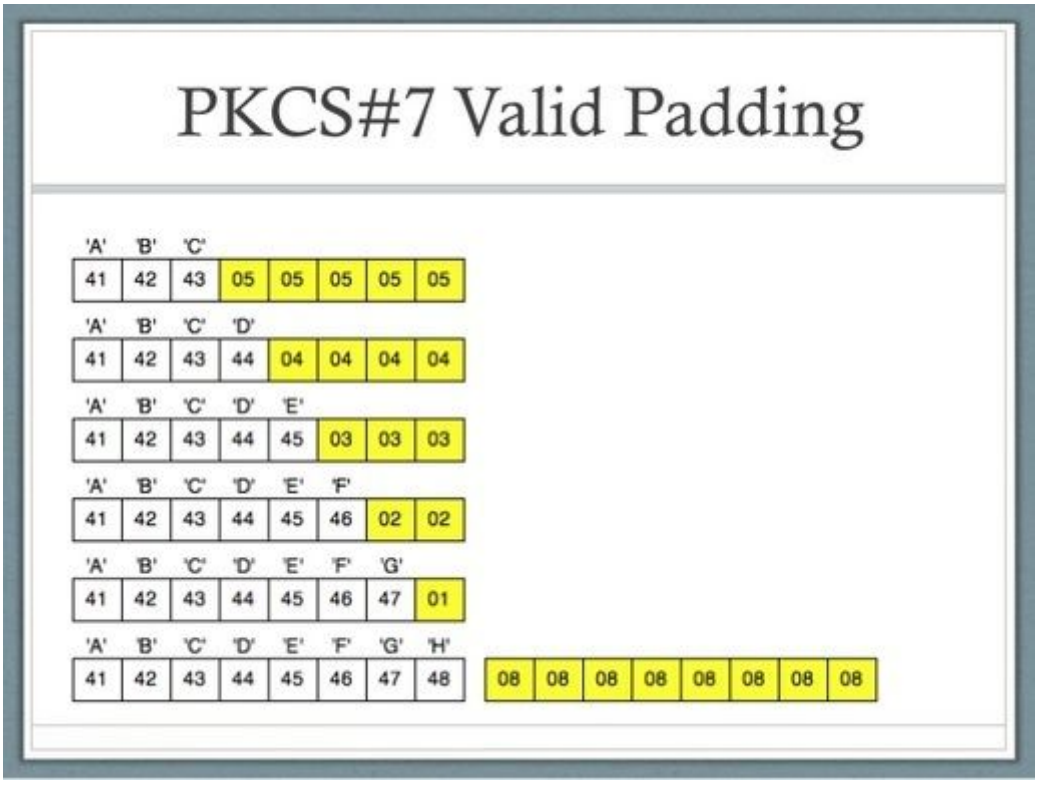
$$C_0 = IV$$

while the mathematical formula for CBC decryption is:

$$P_i = D_K(C_i) \oplus C_{i-1},$$
$$C_0 = IV.$$

Padding

- What happens when the length of the original message is not divisible by the length of the block?
    - i.e. the text does not fit into an exact number of blocks.
- This is where padding comes in.
- Padding is used to fill the remaining bytes in a block where the original message is finished. There are a few different padding schemes but the most common is PKCS7; it appends the value *n* where *n* is how many bytes of padding is required, *n* times.



How the attack works

- Given cipher blocks C_1, C_2 and their corresponding plaintext blocks P_1, P_2, cipher block chaining works like so
    - $C_2 = E(C_1 \oplus P_2)$
    - $P_2 = D(C_2) \oplus C_1$.
- We rearrange the last equation to $D(C_2) = P_2 \oplus C_1$ as this form will be more useful later.
- Suppose we have some function that returns 3 different values depending on the input.

    - These values are, correct, incorrect and incorrect padding.
    - We call this function an oracle.
- Suppose we have a carefully designed cipher block C' such that the oracle tells us that $C'C_2$ is padded correctly.
    - This will decrypt to $P'P_2'$.
    - P' will be garbage plain text and we don't care what that is. It is P_2' that we care about.
    - This is because
        - $P_2' = D(C_2) \oplus C'$
    - but we also know that $D(C_2) = P_2 \oplus C_1$. Hence we can substitute this in to get
        - $P_2' = P_2 \oplus C_1 \oplus C'$.
    - Rearranging we get
        - $P_2 = P_2' \oplus C_1 \oplus C'$.
- We know what C' is since we constructed it and we know what C_1 is since we were given it.
    - What we want to know is P_2.
    - From our oracle we can find out bytes of P_2'.
- Suppose we want to find the last byte.
    - Then what we would do is keep trying different values C' where we only change the last byte.
    - Once we succeed in finding a C' that produces correct padding then we know that the last byte for P_2' is 0x01 because of the PKCS7 padding.
    - Hence we can figure out the last byte of P_2 using the above formula.
- To figure out the second last byte P_2, we want the last 2 bytes of P_2' to be both 0x02 as this is valid padding.
    - To make the last byte of P_2' to be 0x02 we can use the same equation:
    - $P_2 = P_2' \oplus C_1 \oplus C'$ but rearranged to $C' = P_2' \oplus C_1 \oplus P_2$.
    - Since we know the last byte P_2 and C_1 we can xor that with 0x02 to find what the last byte of C' is.
    - Then we keep trying different values for the second last byte of C' until the oracle says that we have correct padding.
    - We then substitute the second last bytes for all the values into our equation $P_2 = P_2' \oplus C_1 \oplus C'$ to find the second last byte of P_2.
- We the repeat this for the third byte and then the fourth byte and so on.
- The attack exploits the information leak given by the padding oracle. In a real world application, this would usually be a web server which creates an error when given invalid input.

How to stop it

This attack can be stopped by implementing simple prevention methods such as:

- Limiting the requests a client can make in a certain time frame to prevent flooding the server with requests
- Get rid of the information leak all together by using a different padding method (that simple)

Additional Resources

Sun Tzu - The Art of War (Summary)

Detail Assessment and Planning - w.r.t. the strategy, weather, terrain, leadership and management

- "All warfare is based on deception"
- "... many calculations lead to victory, and few calculations to defeat"

Waging War

- understand the economy of warfare - the provisions needed, the expenses of the behind and at the front-lines
    - prolonged warfare drains the troops and the country
- limit the cost of competition and conflict - make use of captured enemy resources

Strategic Attack

- the source of strength is unity, not size
- in order of importance, the factors of success: attack, strategy, alliances, army and city
    - "the skillful leader subdues the enemy's troops without any fighting"
- Know yourself and know your enemy

Disposition of the Army

- Defend existing positions until a commander is capable of advancing from those positions in safety
- Recognise strategic opportunities - "the opportunity of defeating the enemy is provided by the enemy himself"
- Try not to create opportunities for the enemy

Forces - use of creativity and timing in building an army's momentum

- "Fighting with a large army under your command is nowise different from fighting with a small one: it is merely a question of instituting signs and signals"
- "The clever combatant looks to the effect of combined energy, and does not require much from individuals. Hence his ability to pick out the right men and utilise combined energy"

Weaknesses & Strengths

- an army's opportunities come from the openings in the environment caused by the relative weakness of the enemy
    - "... the clever combatant imposes his will on the enemy, but not allow the enemy's will to be imposed on him"
    - "Carefully compare the opposing army with your own, so that you may know where strength is superabundant and where it is deficient"
- respond effectively to the changes in the fluid battlefield

Military Maneuvers

- Beware of direct conflict
- But be prepared for and learn to win in those situations
- "Having collected an army and concentrated his forces, he must blend and harmonise the different elements thereof before pitching his camp"
- "When you surround an army, leave an outlet free. Do not press a desperate foe too hard."

Variations & Adaptability

- need for flexibility in army's responses - take into consideration the advantages and disadvantages
- "The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable"

Movement & Development of Troops

- evaluate the intentions of others
- evaluate the different situations an army might be in when it's in new enemy territories and how to respond to them
- build your army well

Terrain

- 3 general areas of resistance: distance, dangers and barriers
- which lead to 6 types of ground positions, each with a set of advantages and disadvantages
- "Regard your soldiers as your children, and they will follow you into the deepest valleys; look upon them as your own beloved sons, and they will stand by you even unto death."

The Nine Battlegrounds - situations (or stages) in a campaign

- " Rapidity is the essence of war: take advantage of the enemy's unreadiness, make your way by unexpected routes, and attack unguarded spots."
- "Carefully study the well-being of your men, and do not overtax them. Concentrate your energy and hoard your strength. Keep your army continually on the move, and devise unfathomable plans."
- "Confront your soldiers with the deed itself; never let them know your design. When the outlook is bright, bring it before their eyes; but tell them nothing when the situation is gloomy. "
- " Success in warfare is gained by carefully accommodating ourselves to the enemy's purpose."

Attacking with Fire

- Have the right weapons when launching an attack
- use of the environment as the weapon
- 5 targets for attack & 5 types of consequences
- "If it is to your advantage, make a forward move; if not, stay where you are. "

- "But a kingdom that has once been destroyed can never come again into being; nor can the dead ever be brought back to life."

Intelligence & Espionage

- Be sure to develop good information sources
- 5 types of intelligence sources
    - "The end and aim of spying in all its five variants is knowledge of the enemy;

Cross-site scripting (XSS)

is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec as of 2007.Their effect may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

DEFINITIONS

In alphabetical order!

- **Asymmetric key cryptography**: Uses different keys for encryption and decryption. Requires only one public and private key per person. Also called public key cryptography.
- **Authentication**: Being able to verify a message came from the owner.
- **Birthday attack**: See Collision attack
- **Birthday paradox**: As long as there are ~24 people, there is more than 50% chance that at least two people share the same birthday (number of pairs grow quadratically as the number of people grows)
- **Bits of security**: a measure of the amount of work needed to decipher a key, or perform an action. Exploiting space/time trade-offs (using more than one computer) halves the number of bits. 128 bits of security is a good ballpark for the universe to end.
- **Broken** (hashing): once a hashing algorithm can be attacked faster than brute force
- **Bug**: Human errors that are in the code (see Vulnerability, Exploit)
- **Certificate Authority (CA)**: trusted entity that issues electronic documents that verify a digital entity's identity on the Internet. The electronic documents, which are called digital certificates, are an essential part of secure communication and play an important part in the public key infrastructure (PKI). Certificates typically include the owner's public key, the expiration date of the certificate, the owner's name and other information about the public key owner
- **Cipher**: a secret way of writing to ensure confidentiality
- **Collision attack**: if you find two messages m1 and m2 that have the same hash h(m)
- **Confidentiality**: Being confidential and private. Everyone can feel and see the system but only one person can do something with it, e.g. Japanese puzzle boxes.
- **Confusion**: the relationship between the key and ciphertext is mysterious (see Diffusion)
- **Crypto literacy**: coming up with cryptography systems that work like magic
- **Diffie-Hellman Key Exchange**: See Module 3

- **Diffusion**: the relationship between the plaintext and the ciphertext is mysterious. If someone changes one bit of the plaintext, we want at least half of the ciphertext to change. (see Confusion)
- **Discrete Log Problem**: g^a mod m = x - given g, m and x, finding a is very difficult.
- **Entropy**: the amount of chaos in a particular thing, e.g. a ciphertext
- **Exploit**: taking advantage of a vulnerability
- **Feistel network**: see Module 6
- **Hashing**: A way of ensuring that a message has **integrity** (has not been tampered with) and this follows with **authentication** (message comes from owner)
- **Intangible** (asset): an asset that is hard to value, e.g. employer morale, consumer information, service availability
- **Integrity**: Being able to make sure a message is impossible to tamper with.
- **Kerckhoff's Principle**: A cryptosystem should be secure even if everything except the key is public.
- **Key Distribution Problem**: Distributing keys in public or over the internet is difficult as it must be done face to face. Public Key Infrastructure (see Assymetric key cryptography) solves this as a person can easily create a key pair and only share the public key.
- **Length Extension Attack**: because most hashes are iterative and take part by part to hash, so you could add to the end of a hash and modify its message.
- **Lucifer**: a block cipher used by banks to transmit data. See Module 6
- **National Vulnerability Database**: a database of common vulnerabilities and exposures. Each one is a year and a number.
- **Nonce**: a number used once that prevents replay attacks, e.g. the time of day
- **Reversibility**: A special cryptographic hash is *not* needed to assure that hash results do not expose the original data: When the amount of information hashed is substantially larger than the internal state or the amount of state ultimately exposed, many different data sequences will all produce the exact same hash result (again, "collision"). The inability to distinguish between the data sequences and so select "the" original is what makes a hash one way. This applies to all "reasonable" hash constructions independent of whether they are "cryptographic" or not. In fact, we can better guarantee the collision distributions when we have a relatively simple linear hash than if we must somehow analyze a complex ad hoc cryptographic hash. On the other hand, when *less* information is hashed than the amount of revealed state, the hashing may be reversible, even if the hash is "cryptographic." And, again, that is independent of the strength of the hash transformation.

- **Perfect secrecy/Perfect forward secrecy**: If you learn a shared secret of another person, everything in the past is safe and past messages and data remain encrypted. Usually this is achieved using a nonce - but often things do not have PS/PFS (e.g. S/Key).
- **Pre-image attack**: if given the hash h(m), you find the message m
- **Public key cryptography**: see Asymmetric key cryptography
- **Reconnaissance (recon)**: gathering information and learning about a target
- **Replay Attack:** sending again a previously intercepted message containing a validated and accepted key.
- **Rick Rescoria**: found the evacuation procedures for the World Trade Centre inadequate – trained and drilled his company's employees on evacuation and successfully orchestrated the evacuation of 2,000 people when the plane crashed.
- **Risk**: A term used in reasoning about what *might* happen, typically with negative outcomes. This is in contrast to evidence, which is used when reasoning about what *did* happen.
    1. An **event that could happen**, e.g. hazard
    2. The **probability** of an event happening (best, worst, average cases)
    3. The **value of assets that could be lost** or at risk
    4. The **expectation of loss** - the probability multiplied by loss value
    - In cryptography, risk is used with respect to probability a cipher may or will be broken by attackers. But, nothing can be known about such risk - there is no way to find the probability - so we say **cipher breaks are always possible**.
    - Risk is about **potential loss**. When we have a choice, the very idea of placing something at risk makes no sense at all unless there is a reward to be gained. All risks (and costs) of a bad outcome need to be seen in the context of the potential *benefit* to be obtained from the desired outcome.
- **Second pre-image attack**: given both the message m1 and hash h(m), you find an m2 with the same h(m)
- **Side channel attack**: looking at metadata to attack a system, e.g. monitoring the power supply
- **Stack canaries**: a tamper seal before a return pointer – to overwrite the return pointer, you also have to overwrite the canary value, which is random
- **Symmetric key cryptography**: A secret key between two parties. This means that if there are 10 people, you'll need 10! keys.
- **Tamper-evident**: **knowing** that someone interfered or altered something.
- **Tamper-proof**: **preventing** someone from interfering or altering something.

- **Tangible** (of an asset): an asset that is physical or visible (money or lives) as opposed to intangible (reputation)
- **Type I and Type II errors**: false positives (type I) and false negatives (type II). When something is actually true but the test says it is false, or something is actually false but the test says it is true.
- **Vulnerability**: a potential flaw or weakness (see Bug, Exploit)
- **Variable Block Cipher:**
    - A variable size block cipher is indefinitely extensible and has no theoretical block size limitation;
    - A true variable size block cipher does not require additional steps (rounds) or layers to approach overall diffusion as the block size is expanded.
- **VENONA:** The NSA codename for a project which broke a hand cipher system used between the Russian KGB or GRU and their operatives in the United States from 1939 to 1946. That cipher system included a one time pad component, which is often considered to be proven unbreakable. The security failure of that system resulted in the *death by execution* of Julius and Ethel Rosenberg. VENONA has its own pages at http://www.nsa.gov/docs/venona/.
- **Voltage Controlled Oscillator:** An oscillator in which the frequency can be controlled over some range by varying a control voltage.
- **White Noise:** A random-like signal with a flat frequency spectrum, in which each frequency has the same magnitude. As opposed to pink noise, in which the frequency spectrum drops off with frequency. White noise is analogous to white light, which contains every possible color. Also see noise and the usual white noise sources thermal noise and shot noise.
- **Zeroize:** The military term for erasing a key from equipment.