Risk

Is/ought = fact / should be that way. Ought is often a moral/ethical question

Risk is invisible. You don't know you took a risk unless it goes wrong. *Risk* is always *bad regardless* of whether it happens or not. you can't see the intelligence behind it but you see the outcomes.

Humans are bad at assessing risk due to the *low probability* of it happening. When estimating risks we tend to evaluate the risks that we are secure against, it is hard to get an accurate picture of the actual probability of it happening. For example, if you were to get your laptop fixed at a shop, there may be a 1/100 chance of the repair destroying your laptop. To the unlucky 1 person, that chance seems to be 100%. Only through repetition repair destroying your laptop. To the 99 out of 100 people who didn't have their laptop destroyed, the chance of repair destroying your laptop seems to be 0% because it didn't and more experiences can we get a more accurate representation of risk. Allocate your resources appropriately across risks.

Humans assess risk based on intuition and past experiences. From Skinners' Pigeon Experiment, observers of the pigeons found that pigeons develop superstitious behaviour, believing in acting in a particular way or committing a certain action, food would arrive. Humans are bad at making decisions about risk based on so called "past life experiences" - it's difficult to evaluate if an event is low probability, because most likely you won't have observed it. Statistically, people underestimate low probability events, because it's unlikely past experience accurately estimates the actual probability.

Richard told a story about when he was on the Eastern Suburbs train line. (Feel free to add details if you remember) The gist was that the train stopped and the lights went out, and the train driver announced that there would be a delay of an indeterminate amount of time. Then he just talked about identifying the different risks of having a train sitting still with no power.

Low-probability high-impact event e.g. asteroids. We tend to obsess about such events or ignore it.

Past experience usually underestimates low probability events

- But we don't care about low probability events unless they are high impact

- Risk is invisible
    - You don't realise you've taken a risk until things go wrong
    - We usually only punish people when the risk goes wrong
        - This shouldn't matter, the fact that the risk was taken is enough
    - You don't see the risk, only the outcome
- Humans are bad at assessing risk
    - We lack the resources to eliminate risk

    - Sanity check the amount of effort placed into each risk

Risk matrix – 2D graph. Impact vs likelihood. Helpful for allocation of resources. High impact and high likelihood (focus). Low impact and low likelihood (ignore). The other ones are trickier.

Risk registers – tool for documenting risks and actions to manage each risk

Compliance – involves ability to demonstrate something

- Prevents forgetting things that need to be done
- Sets a minimum standard
- Unlikely policies to comply with are good enough to deal with present risks
- *Compliance Culture*

Measure info in bits:

1 bit of info distinguishes between two cases

2 bits -> 4 cases

- Bits of security - a cipher takes n operations to solve. This can be written in terms of 2^x where x is the number of bits of security required to solve a problem

Centralisation – Systems with a single point of failure often have very high-level security, but if it goes down it has a huge impact.

Space-time tradeoff – is the case when an algorithm/program can increase space usage to decrease time spent or vice versa

- Exploiting space-time tradeoff, an attacker can roughly halve the effective number of bits.

Work factor – work factor is defined as the amount of effort required to break down a cryptosystem

- Increase the amount of work for someone to do a bad thing so that it's not profitable

Dealing with Risk

1.Prevention

Try to prevent an event from happening by removing the vulnerabilities which allow the event to occur. I.e. if a fire is likely to occur in a building because people smoke in the building, then implement rules to prevent people from smoking inside the building.

2.Limitation

If the event cannot be prevented, then try and minimise it by limiting how bad the situation can get. I.e. if a fire does happen to occur inside a building, a method of limitation would be the installation of fire separation walls beforehand, so that the effect of the fire is limited to certain areas. Another method of limitation is by lowering the probability of the event occurring if the event cannot be fully prevented.

3.Passing the risk to a 3rd Party
Similar to Limitation, we try and limit the effects of the risk by shifting the responsibility off to another party. I.e. we can limit the losses occurred from the fire by having insurance, which can help with the recovery from the fire, through financial aid.

4.Wearing the risk
If a risk cannot be fully prevented, it is necessary to just wear the risk and in the case that the bad event does happen, the methods used to minimise the impact will help reduce the severity of the risk so that the worst case scenario does not occur.

Public Key Cryptography

The **problem** with private key cryptography is that if a person wanted to communicate with n people, they would need a key for each pair of people (10C2 people, so in the order of n^2)

How would these keys be established in the first place, *infeasible to pre-exchange keys*

Ralph **Merkle** proposed Secure Communications over Insecure Channels

Merkle Puzzles

Alice gives Bob 1000 sealed envelopes, with each containing a key and an identifier. Bob opens a random envelope and tells Alice the identifier for this envelope. Alice can then look this up in her list and now they can send messages using the key.

For an attacker, then would have to brute force all 1000 (on average 500) envelopes to find the one which contains the identifier they are using.

RSA

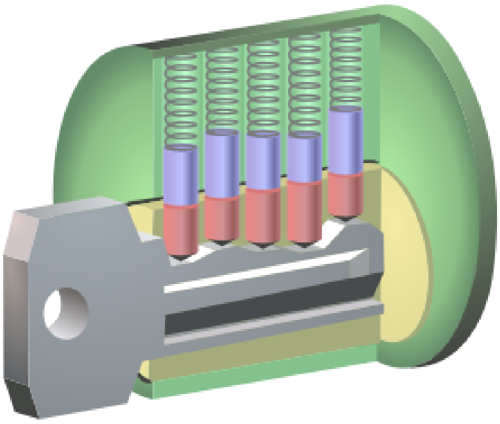
RSA was a revolutionary system as it is the first instance of public key cryptography
- 2 keys, one public and one private
- *Public* one can be *shared* to everyone that wants to send a message
- *private* is *retained* by the person receiving the messages.
- The *two keys* are *mathematically related*
- Only the person with the *private* key can *decrypt* the messages
- RSA is based on modular arithmetic (ie A^B mod C = ((A mod C)^B) mod C)
- Decode key is kept secret, therefore we only need to keep 1 secret instead of say n2 keys

Calculating RSA

1. Message M has numerical equivalent ‘m’
2. Choose p,q to be different primes (LARGE)
3. Calculate $n = pq$
4. Calculate $\Phi(n) = (p-1)(q-1)$
5. Choose an integer ‘e‘ such that $0 << e << p,\ q$ and $gcd(e,\ \Phi(n)) = 1$ (relatively prime / coprime)
6. Choose an integer ‘d such that $e \cdot d \equiv 1\ mod\ \Phi(n)$
    a. Can be done by brute force
7. Encoding m:
    c → m^e mod (n)
8. Decoding c:
    m → c^d mod (n)
9. Receiver makes n and e public (and keeps p, q, d private)

A link to dropbox file on Public Key Cryptosystems and RSA:
https://www.dropbox.com/s/ykk1c6n1u6w6086/RSAandPublicKeyCryptography.pdf?dl=0

Lock Picking



When the correct key is inserted, the gaps between the key pins and driver pins align with the edge of the plug, called the shear line.

Methods:

Lock bumping

-
- Bump key inserted one notch short of full insertion. The key is 'bumped' inwards to force it deeper into the key way. A small force is transmitted to all the key pins. If a light rotational force is applied during the slight impact, the cylinder will turn.
- Tension wrench (pin tumbler lock picking)
  - Applies torque to the plug of a lock to hold picked pins in place. Once all pins are picked, the tension wrench is used to turn the plug and open the lock

Rake picks

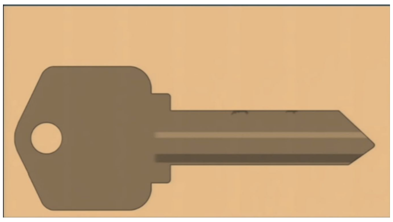
- Rapidly slide the pick past all the pins to bounce the pins until they reach the shear line
-

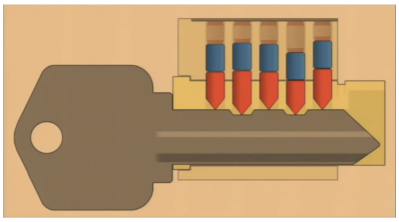
Shim

- Thin piece of metal, slide it into the shackle housing and pull it from side to side (inserted into the top of the lock, not through the keyhole)
-

Key impressioning

- Starting with a flat or ‘blank’ key, fashion the key into the shape of the lock





- Don’t need anything but hands and the lock, but filing the key can help

Other

- Inserting a card in gap of a door.