Information Security Training

Information Security and Cryptography

2018-05-21 - ThaiNOG

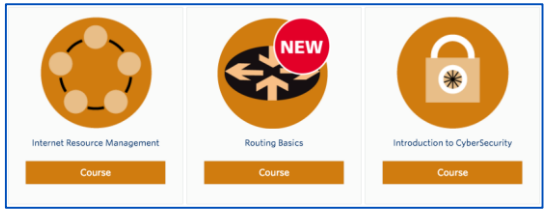
APNIC

Introductions

- Jamie Gillespie
  - jamie@apnic.net
  - Security Specialist @ APNIC
  - Community engagement, CERT building, InfoSec training, awareness

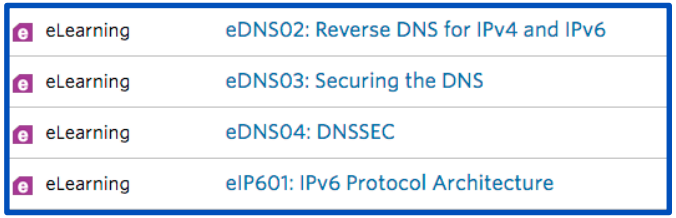
  - Work history
    - 8 years at AusCERT, Australia's national CERT (at the time)
    - Google
    - Macquarie Telecom / Cloud Services
    - before all that, a few roles at UUNET (a backbone ISP in Canada)

eLearning – Free to the public



APNIC Academy

apnic.academy



Web classes

training.apnic.net/courses

YouTube

youtube.com/APNICTraining

Stay up-to-date
https://mailman.apnic.net/mailman/listinfo/training-announce

Coming Soon!


Take the
APNIC Survey 2018
YOU COULD WIN...
We want to hear from you about APNIC's services and the needs of the Community
Opens 28 May
Microsoft Surface Pro 4
An Apple Watch Sport
Virtual gift cards

Next Conference

Register now!

https://conference.apnic.net/46/register/register

APNIC 46

Fellowships

Applications open 7 May

https://conference.apnic.net/46/fellowship

NOUMEA, NEW CALEDONIA

6 – 13 September 2018

Save the date - APNIC 48

Chiang Mai, Thailand
5-12 September 2019

Hosted by

THNIC
มูลนิธิศูนย์สารสนเทศเครือข่ายไทย
THAI NETWORK INFORMATION CENTER FOUNDATION

TISPA
สมาคมผู้ให้บริการอินเทอร์เน็ตไทย
Thai Internet Service Provider Association

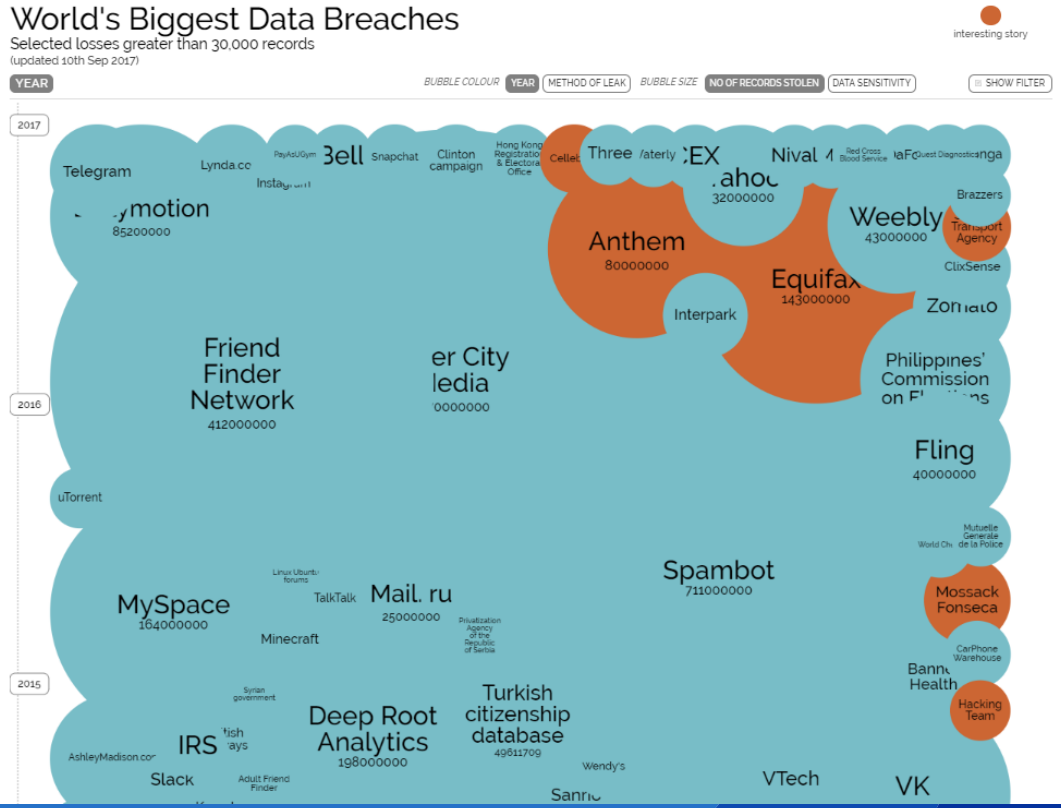
Information Security Training

Information Security Overview

Information Security

- Definition:
  - the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information
- The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimizing the impact of security incidents
  - This is done through Prevention, Detection, and Recovery
- Information, IT, Internet, Cyber… it's all Security

Security Breaches

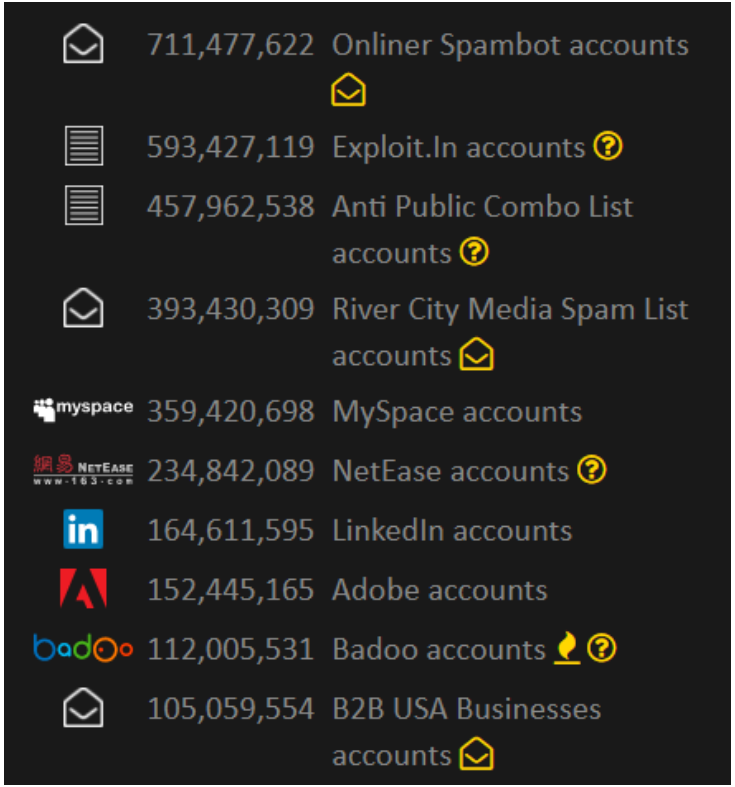


Ref:
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Shortened: https://goo.gl/P1279w

Security Breaches

- haveibeenpwned.com tracks accounts that have been compromised and released into the public
  - 235 pwned websites
  - 4,739,264,622 pwned accounts
  - 55,852 pastes
  - 53,076,361 paste accounts



Security Breaches

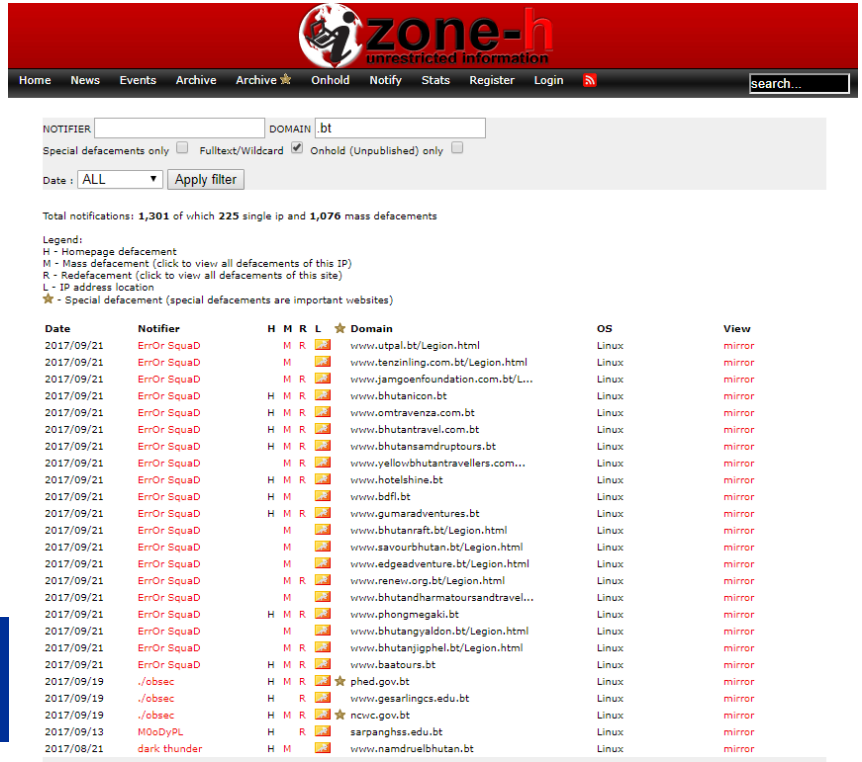
- zone-h.org/archive tracks and archives website defacements

Date	Notifier	H	M	R	L	Domain	OS
2017/09/18	Prosox	H				cain.larc.nasa.gov	Linux
2017/09/11	GuardIran Security Team					data.howardcountymd.gov/Test/	FreeBSD
2017/09/09	SynthDeathcore			R		cantontwp-oh.gov/synth.htm	Linux
2017/08/24	jok3r					www.mrcog-nm.gov/king.htm	Linux
2017/08/22	Mr.Kro0oz.305		M	R		www.unicoicountytn.gov/Krooooo...	Linux
2017/08/22	Mamad Warning					hip.phila.gov/index.html	Win 2008
						www.sealbeachca.gov	Win 2008
						cascade.lbl.gov/wp-content/upl...	Linux
			M			assessment.nnva.gov	Win 2008
				R		www.dickinsoncountymi.gov/imag...	Win 2008
			M			www.documents.guam.gov	Linux

hacked by proxy ~~ guardiran security team

Hello Admin , i am White hat hacker , i am here just for help to you !

i Patched your Vulnerability ;) , now you can delete This html Page. Good Luck Partner <3



Security Breaches

- Common vulnerabilities can lead to mass compromises

January 08, 2008

Mass SQL injection attack compromises 70,000 websites

Updated Wed., Jan. 9, 2008, at 4:37 p.m. EST

An automated SQL injection attack, which at one point compromised more than 70,000 websites, hijacked visitors' PCs with a variety of exploits last week, according to researchers.

Coordinated Website Compromise Campaigns Continue to Plague Internet

Martin Lee - March 20, 2014 - 18 Comments

Memcached DDoS: The biggest, baddest denial of service attacker yet

Distributed denial of service attacks just got turned up to 11 with Memcrashed, an internet assault that can slam a website with over a terabyte of bad traffic.

InfoSec Definitions

- Let’s start with definitions so we speak a common language
- **Asset** - what we are trying to protect
  - The “information” part of “information security”
  - Resources
    - Physical – servers, routers, switches
    - Virtual – CPU, memory, bandwidth, network connections

InfoSec Definitions

- **Threat** - a circumstance or event with the potential to negatively impact an asset
  - Intentional
    - Hacking, malware, DDoS, company insiders, theft
  - Accidental
    - Malfunction, user error
  - Natural
    - Natural disaster, earthquakes, storms/floods

InfoSec Definitions

- **Vulnerability** - weakness in an asset's design or implementation
  - Software bugs
    - Most vulnerabilities you'll hear of fall into this category, OS's, applications, services
  - Protocol "bugs" or design flaws
    - SYN flood, predictive sequence numbers, ASN.1, NTLM
  - Misconfigurations
  - Insecure authentication
    - Weak passwords, lack of 2FA/MFA
  - Unvalidated inputs
    - SQL injection, Cross Site Scripting (XSS)
  - Poor physical security
    - Example on next slide…

InfoSec Definitions

- **Risk** – the potential for loss or damage to an asset caused by a threat exploiting a vulnerability
- Sometimes shown as:
  Risk = Threat x Vulnerability
- Or a more detailed view is:
  Risk = Asset (or Impact) x Threat x Vulnerability

InfoSec Definitions

The brazen airport computer theft that has Australia's anti-terror fighters up in arms

By Philip Cornford
September 5, 2003

On the night of Wednesday, August 27, two men dressed as computer technicians and carrying tool bags entered the cargo processing and intelligence centre at Sydney International Airport.

They presented themselves to the security desk as technicians sent by Electronic Data Systems, the outsourced customs computer services provider which regularly sends people to work on computers after normal office hours.

After supplying false names and signatures, they were given access to the top-security mainframe room. They knew the room's location and no directions were needed.

Inside, they spent two hours disconnecting two computers, which they put on trolleys and wheeled out of the room, past the security desk, into the lift and out of the building.

InfoSec Definitions

- **CVSS** – Common Vulnerability Scoring System
  - A system to translate the characteristics and impacts of a vulnerability into a numerical score
  - Interactive calculator is at https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- The Apache Struts vulnerability in 2017 scored a perfect 10

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Impact Score: 6.0
Exploitability Score: 3.9

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed
Confidentiality (C): High
Integrity (I): High
Availability (A): High

InfoSec Definitions

- **Mitigate** – to reduce the seriousness or severity
  - This is done by applying **security controls**
  - Controls can be classified by their time of impact:
    - Preventative
    - Detective
    - Corrective
  - or by the type of control:
    - Legal and regulatory compliance
    - Physical
    - Procedural / Administrative
    - Technical

InfoSec Definitions

- **Defence In Depth** – the layering of security controls to provide redundancy in case of a failure or vulnerability
  - These commonly layer controls at different times and types (see prev)
  - Sometimes referred to as a Castle Approach

For more castle defences, see http://tvblogs.nationalgeographic.com/files/2013/08/Castle-Traps-and-Defenses.jpg

Pictured to the left is Caerphilly Castle https://commons.wikimedia.org/wiki/File:Caerphilly_aerial.jpg

InfoSec Definitions

- **Defence In Depth**
- Discuss: Imagine you had a bar of gold to protect
  - What container would you put it in?
  - What room would the container be in?
  - What locks are on the doors?
  - Where is the room located in the building?
  - What cameras are watching the room and building?
  - What humans are watching the cameras?
  - Who will respond with force to a theft attempt?
  - Bonus question: How much did all of this cost?

InfoSec Definitions

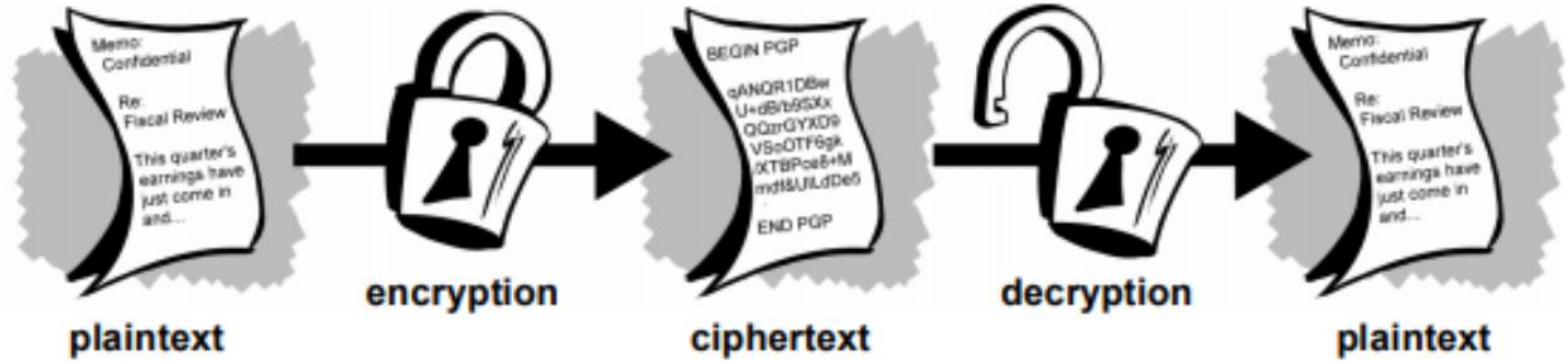
- **Threat actor** – a person trying to cause harm to your system or network
  - Commonly called an attacker or hacker, although the definition of a hacker has changed over many years
  - Also known as **malicious actor**
  - Can be further broken down into categories such as:
    - Opportunistic
    - Hacktivists
    - Cybercriminals (organized or not)
    - Nation States / Government Sponsored
    - Insiders (intentional or accidental)

Information Security Training

Cryptography

Cryptography

- Terminology



  - Cryptography
    - From Greek, “crypto” meaning hidden or secret, “graphy” meaning writing
  - Cryptanalysis
    - From Greek, “crypto” meaning hidden or secret, “analysis” meaning to loosen or untie

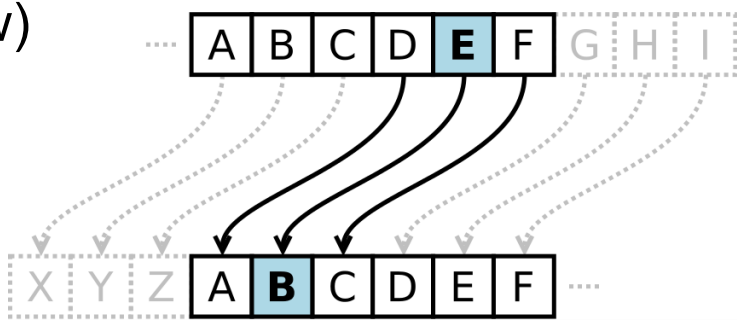
Cryptography

- History
  - Non-standard hieroglyphs in Egypt (1900 BCE)
  - Modified words on clay tablet in Mesopotamia (1500 BCE)
  - Monoalphabetic substitution ciphers
    - Hebrew scholars using Atbash Cipher (500-600 BCE)
    - Indian authors of Karma Sutra document ciphers for messages between lovers (400 BCE to 200 CE)
    - Atbash Cipher:

Plain	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
Cipher	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Cryptography

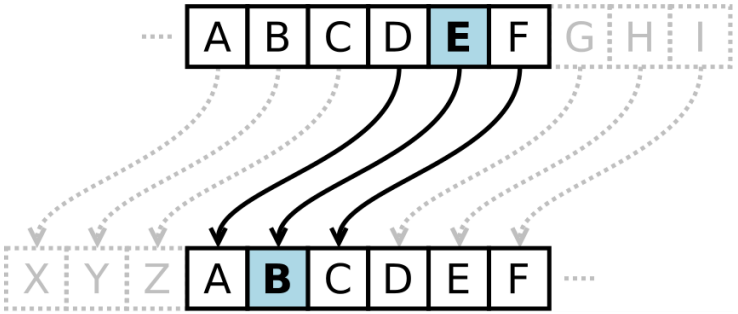
- History
  - Romans used a shift cipher called a Caesar Cipher after it's famous user Julius Caesar (100-44 BCE)
    - He used a left shift of 3 places, known as the key
    - The ROT13 systems uses a shift of 13 places
  - Caesar cipher is also used in secret decoder rings (1930's to now)



Cryptography

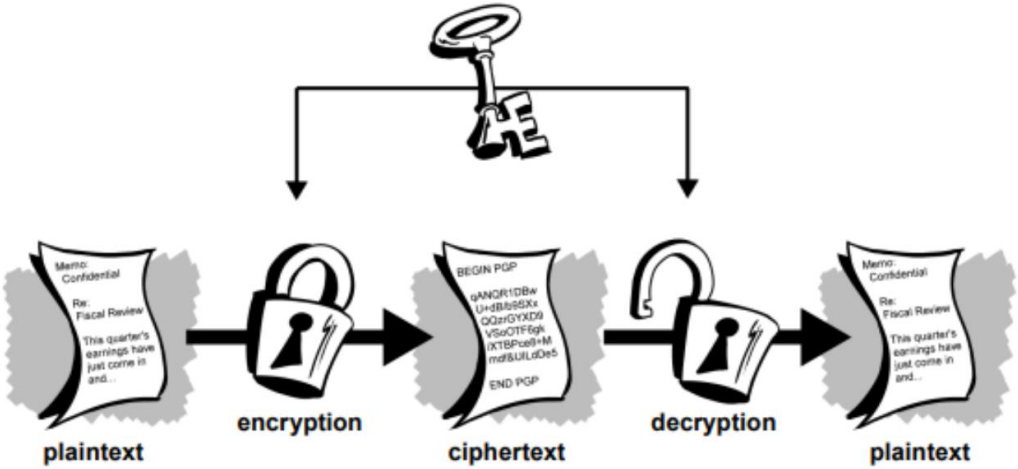
- Exercise: Use Atbash and Caesar ciphers
  - https://gchq.github.io/CyberChef/ (or Google: Cyber Chef)
  - Look under Encryption/Encoding for Atbash and ROT13
  - Using ROT13 for Caesar cipher, left shift encoding is negative numbers (e.g. -3) and right shift decoding is positive numbers (e.g. 3)

  - Decode Atbash: svool dliow
  - Decode Caesar: zovmql fp crk



Cryptography

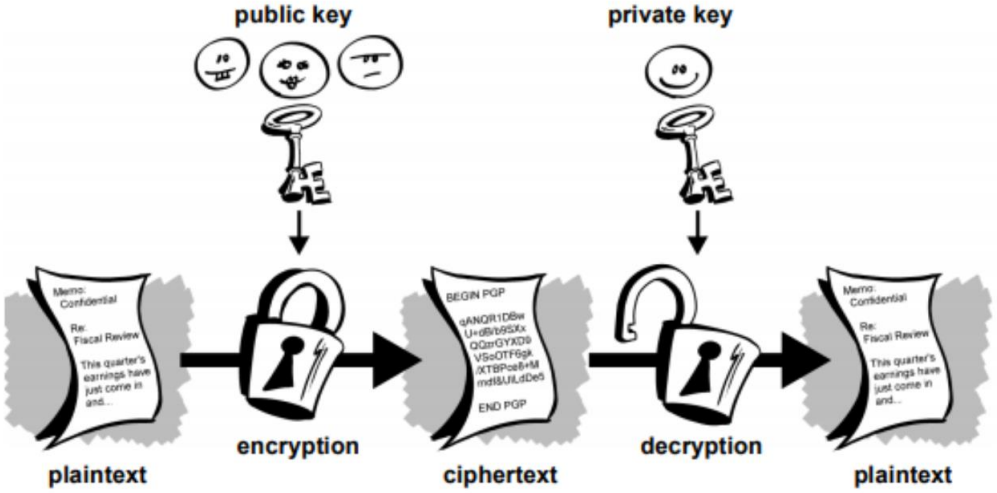
- Symmetric Algorithms
  - aka Private Key Crypto
  - The basic concept
    - Uses the same key



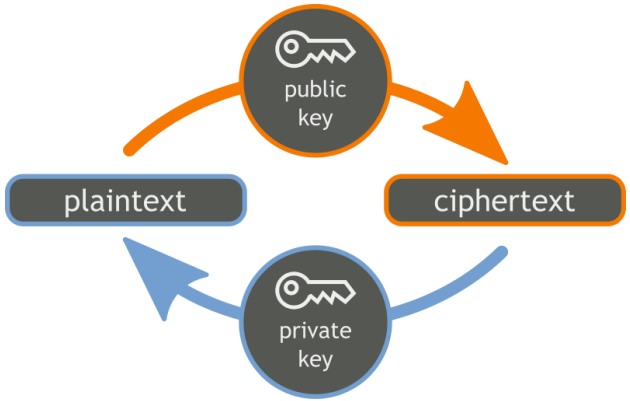
  - Common symmetric algorithms
    - AES
    - DES, 3DES
    - Blowfish
  - Exercise: Using CyberChef again, encrypt/decrypt using Blowfish
    - Demo on-screen

Cryptography

- Asymmetric Algorithms
  - aka Public Key Crypto
  - The basic concept
    - Uses a public key and a private key

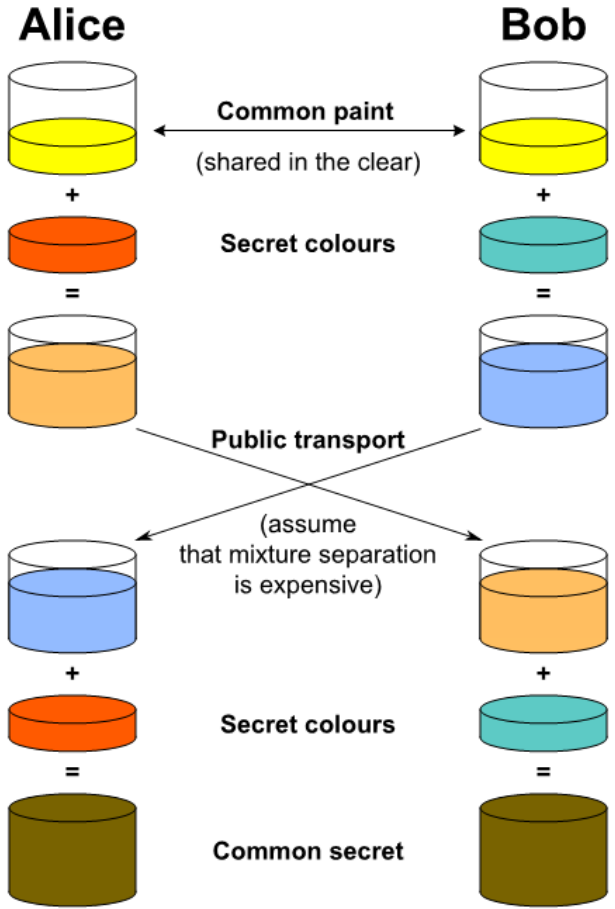


  - Common asymmetric algorithms
    - RSA (shown in the first image)
    - Diffie-Hellman (shown on next slide)
    - ElGamal



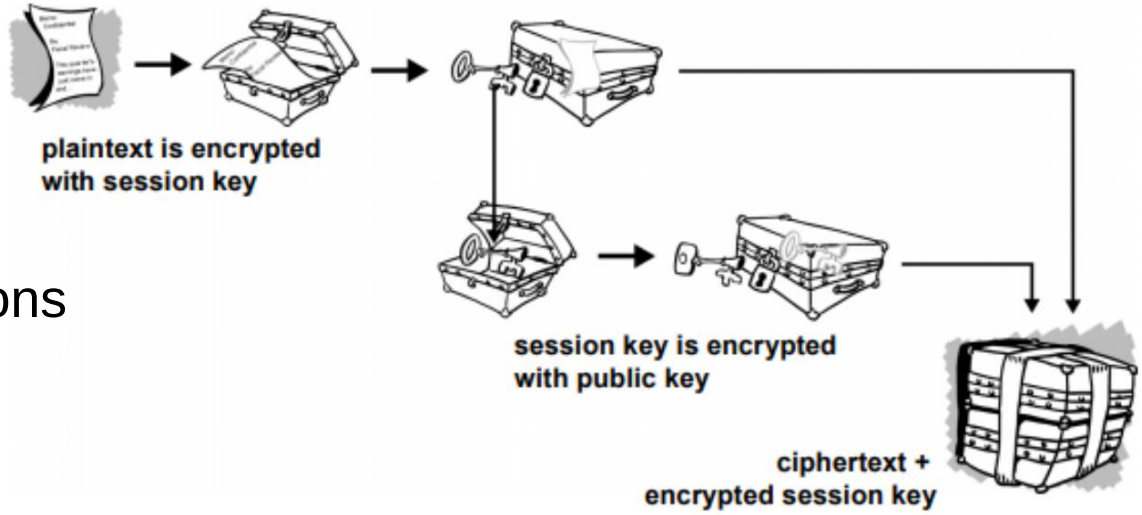
Cryptography

- A simple graphical explanation of how Diffie-Hellman key exchange works



Cryptography

- Asymmetric algorithms are slower than symmetric, so most implementations use a combination of both to ensure it is both fast and secure



  - Common implementations
    - SSL
    - PGP / GPG

Cryptographic Hashing

- Cryptographic Hash Function, aka One-Way Hashing
- The basic concept
  - Take an input of any length, process it in such a way that it is infeasible to reverse, and produce a fixed length output.
  - Example or changing one character produces a very different output
    - **TestNumber1** put through SHA-256 produces the output 541a6d07ae40626b61456912992b38b7e726d121d1eddfe47719cefe6811385e
    - **TestNumber2** also using SHA-256 produces the output 596924bec1ef084d5173fc18c8ae94e6083c08ecee6d57d83eaafcb83b221b3e

Cryptographic Hashing

- Example or changing one character produces a very different output
  - **TestNumber1** put through SHA-256 produces the output 541a6d07ae40626b61456912992b38b7e726d121d1eddfe47719cefe6811385e
  - **TestNumber2** also using SHA-256 produces the output 596924bec1ef084d5173fc18c8ae94e6083c08ecee6d57d83eaafcb83b221b3e
  - EXERCISE - These were generated on a web site implementation of SHA-256, but you can check the same output on your own computers
    - On Linux: `echo -n TestNumber1 | sha256sum`
    - On OS X: `echo -n TestNumber1 | shasum -a 256`
    - Windows needs the PsFCIV tool downloaded from Microsoft
    - Or just use any number of web sites like http://www.fileformat.info/tool/hash.htm

Uses of Hashing

- Password authentication
  - Because the output of a hash is identical for the same input, hashes are commonly used for storing and verifying passwords.
  - When a user creates a new password, the authenticating system stores the hash output (for example, TestNumber1 from the previous slide)
  - When the user logs in later, they supply their password which is put through the same hash function, and the output is compared to the stored output.
  - If the hashes match, then the passwords must match.
  - This has advantages over storing the password in plaintext, in case the server is compromised and the hashes are exposed.

Uses of Hashing

- Verifying file integrity
  - When downloading files from the internet you may see a hash provided.
  - This allows you to put the downloaded file through the same hash and compare outputs.
  - This verifies that the file hasn’t been modified during download, and allows for the file to be available for download from multiple sites while the authoritative web site hosts the hash to be compared against

Uses of Hashing

- Verifying file integrity
  - File Integrity Monitor (FIM) applications also use hashing of files to confirm integrity. This is done through the creation of a database of the hash output from all (or selected) files on a computer, to be compared against later. If any hashes change, the administrator is alerted. FIM systems are used to find modified files from attackers, or changes in configuration files.
  - Exercise: Run sha256sum on a file, edit the file, then sha256sum it again
    - `sha256sum test-file`
    - `nano test-file  or  vi test-file`
    - `sha256sum`

Uses of Hashing

- Proof-of-work
  - BitCoin (and other cryptocurrencies) uses the work to create a partially known hash to prove that the end user (miner) performed the amount of work on their computer. For example, one proof of work is to have a computer try many different input combinations in order to produce an output value that has the first 20 bits being zero.
  - Similar proof of work systems have been created for a way to reduce spam. Legitimate email senders can have their computer perform the proof-of-work function for each email sent, which isn't too onerous for the typical small amount of email sent. Spammers however want to send email much faster and don't have the time or resources to generate the special hash for each email sent.

Cryptographic Hashing

- Types of Hashing Algorithms
  - MD5 – First published 1992 - Deprecated, do not use
    - Produces a 128-bit hash output, usually represented as 32 hex digits
    - 2109494ae833752b82ba786e7a4d7209
  - SHA-1 – First published 1995 - Deprecated, do not use
    - Produces a 160-bit hash output, usually represented as 40 hex digits
    - a316ec9b579abda6cc712490894619f47f38cbef

Cryptographic Hashing

- SHA-2 – First published 2001
  - Consists of 6 hash functions with outputs of 224, 256, 384, and 512 bits
  - The other 2 are SHA-512/224 and SHA-512/256 which are truncated versions of SHA-512 and are not commonly used. Added in 2012.
  - SHA-256 = 541a6d07ae40626b61456912992b38b7e726d121d1eddfe47719cefe6811385e
  - SHA-512 = 04ce124b492943eb9883cb2af654d89e02548e4f11bf5c9dff35217d63cfbed3b3c4125ecc8bf4270566f51c09c84aed21d4891ce2b1eb6bb2e4ccfc25dd9e35
  - SHA-2 functions are partially vulnerable to a type of attack called a “length extension attack”, so if you are currently using SHA-2 you should start looking at moving to SHA-3, bcrypt, PBKDF2, or scrypt. If you are using something weaker than SHA-2 you should skip SHA-2 and move to something stronger.

Cryptographic Hashing

- PBKDF2, bcrypt, scrypt, Argon2
  - I'm grouping these together as they all work on a similar basic principle.
  - For input you provide the plaintext password, a salt, and the number of iterations.
    - A salt is a random block of random characters that is prepended or appended to the plaintext password, thus making the password stronger before being put through the hash function
      - Salt can be added to other hash algorithms (e.g. SHA-1, SHA-256) to make them more secure.
      - Salts should be used and changed for each password being stored, so that 2 users with the same password won't have the same hash output.

Cryptographic Hashing

- PBKDF2, bcrypt, scrypt, Argon2
  - For input you provide the plaintext password, a salt, and the number of iterations.
    - Iterations are the number of times the hash function is performed before the output it stored. Remember the basic premise of hashes: going forwards is easy, going backwards it extremely difficult.

Cryptographic Hashing

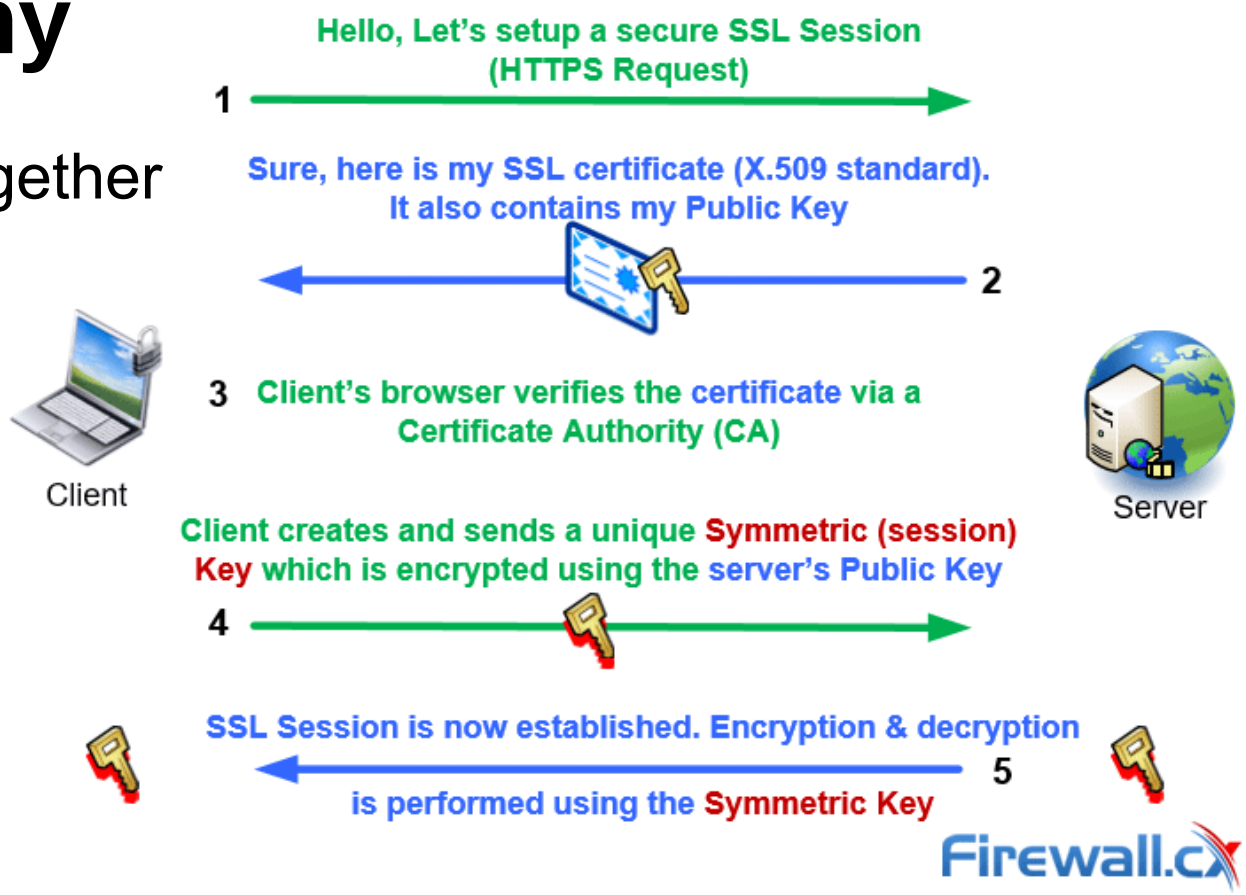
- PBKDF2, bcrypt, scrypt, Argon2
  - PBKDF2 (Password-Based Key Derivation Function 2) and bcrypt are older and more trusted, but use a fixed amount of memory to execute.
  - Scrypt is newer (so less trusted) but require larger amounts of memory, thus making it harder to attack using custom hardware or GPUs.
  - Argon2 was chosen as the winner from the Password Hashing Competition and is similarly resistant to attack using GPUs, but is also a newer algorithm and hasn't been tested or trusted as much yet.
    - Ref: https://password-hashing.net/

Cryptography

- SSL / TLS
  - Certificates issued as part of a Public Key Infrastructure (PKI) with a hierarchical structure of Certificate Authorities (CA) and Intermediate CAs
  - Not discussed here is the key exchange, but you can reach more at
    - https://en.wikipedia.org/wiki/Key_exchange
    - https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange (includes a nice graphic to help you make sense of it, see next slide)
    - Think about it like a box with 2 locks…

Cryptography

- How it's all put together
  - SSL / TLS



Cryptography

- PGP
  - Each user creates their own certificate/key-pair and uses a web-of-trust model
  - Web-of-trust benefits from users signing each others' public keys, usually after verifying the person's identity and public key ID in person
  - Exercise: Create a PGP key pair
    - https://pgpkeygen.com/

- Reminder, the private key is supposed to be kept private

Cryptography

Adobe accidentally releases private PGP key

The firm's security team failed in a spectacular fashion.

By Charlie Osborne for Zero Day | September 25, 2017 -- 08:35 GMT (16:35 GMT-08:00) | Topic: Security

```
LJyYLUvFjL3i3jbiNT1NKldwqaL2i9OuRAuHthoFGOKIqr6hmtOYzUem/cl+
ZlRwd77Vmfc=
=QOc7
-----END PGP PUBLIC KEY BLOCK-----

-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

xcaGBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDEmS0F9MRZIcV0UKyA5qV
```

Archived copy of the original leak is at: http://archive.is/h7qQ2

Attacks Against Cryptography

- Rainbow tables
  - Hashing algorithms create a fixed length output.
  - What if you pre-compute hashes for all known inputs (e.g. passwords 1-8 characters long, with upper/lower case letters and numbers). Then when you are presented with a hash, you can look it up to see what the plaintext input is.
  - Now you're got a Rainbow Table!
    - Note: rainbow tables are actually more complex, but the above description is good enough

Attacks Against Cryptography

- Rainbow tables
  - Generating rainbow tables requires a lot of computer effort, and a moderate amount of storage. But once created, they can be used again and again (and shared)
    - 1-8 characters long, using a-z.A-Z.0-9 = 127GB
      - Keyspace is 221,919,451,578,090 (221 trillion)
    - 1-9 characters long, using a-z.A-Z.0-9 = 690GB
      - Keyspace is 13,759,005,997,841,642 (13.8 quadrillion)

Cryptography

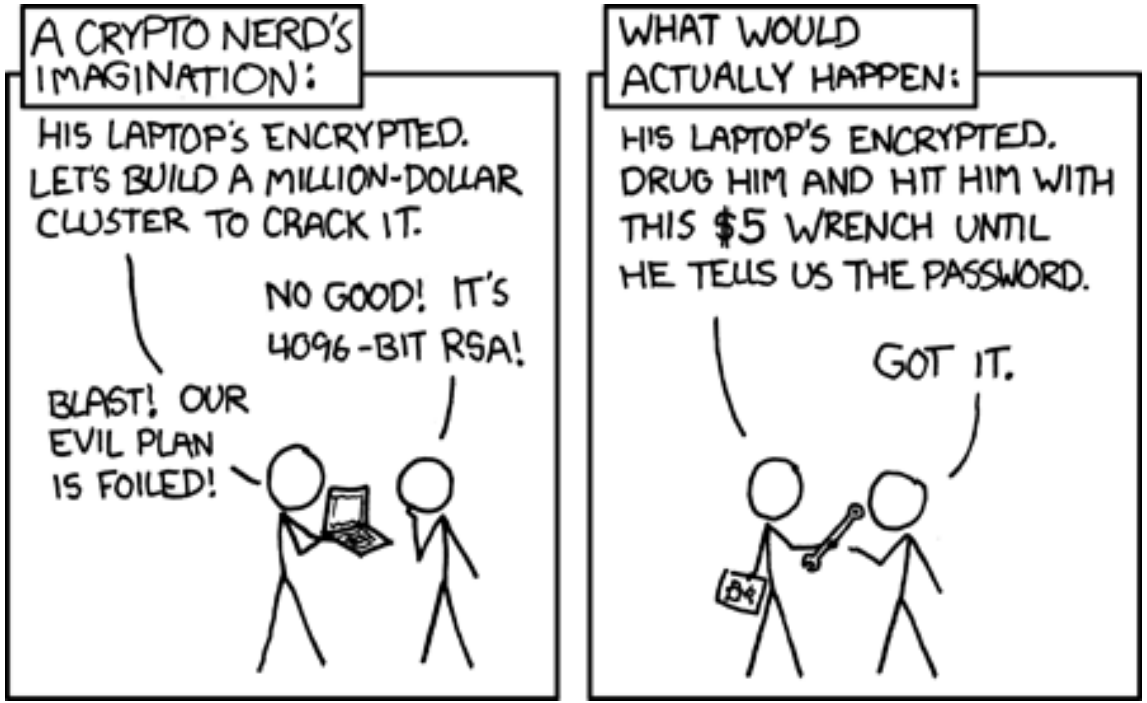
- Brute-force
  - If you have a fast-enough computer, you can just try running every possible input through an algorithm and seeing the output matches the ciphertext or hash you're trying to break.
  - CPUs have gotten faster, but GPUs with 100's of cores are faster
  - Brute force attacking a RAR file
    - 64 passwords per second using Intel Xeon E5 2603
    - 25,300 passwords per second using NVIDIA GeForce GTX 1080
    - Ref: https://www.elcomsoft.com/edpr.html

Cryptography

- Brute-force
  - Combine 10 x GTX 1080 Ti's in one machine and you can do the following:
    - SHA-1 – 113.5 billion hashes per second
    - SHA-512 – 15 billion hashes per second
    - SHA-3 – 11.7 billion hashes per second
    - MSSQL (2012, 2014) – 14.2 billion hashes per second
    - bcrypt – 218.9 thousand hashes per second
    - All this for $16,500 USD (not including the massive power bill for burning 4 kilowatts of power!)
    - Ref: https://www.servethehome.com/deeplearning11-cracking-passwords-with-10x-nvidia-geforce-gtx-1080-ti-gpus/

Cryptography

- Brute-force

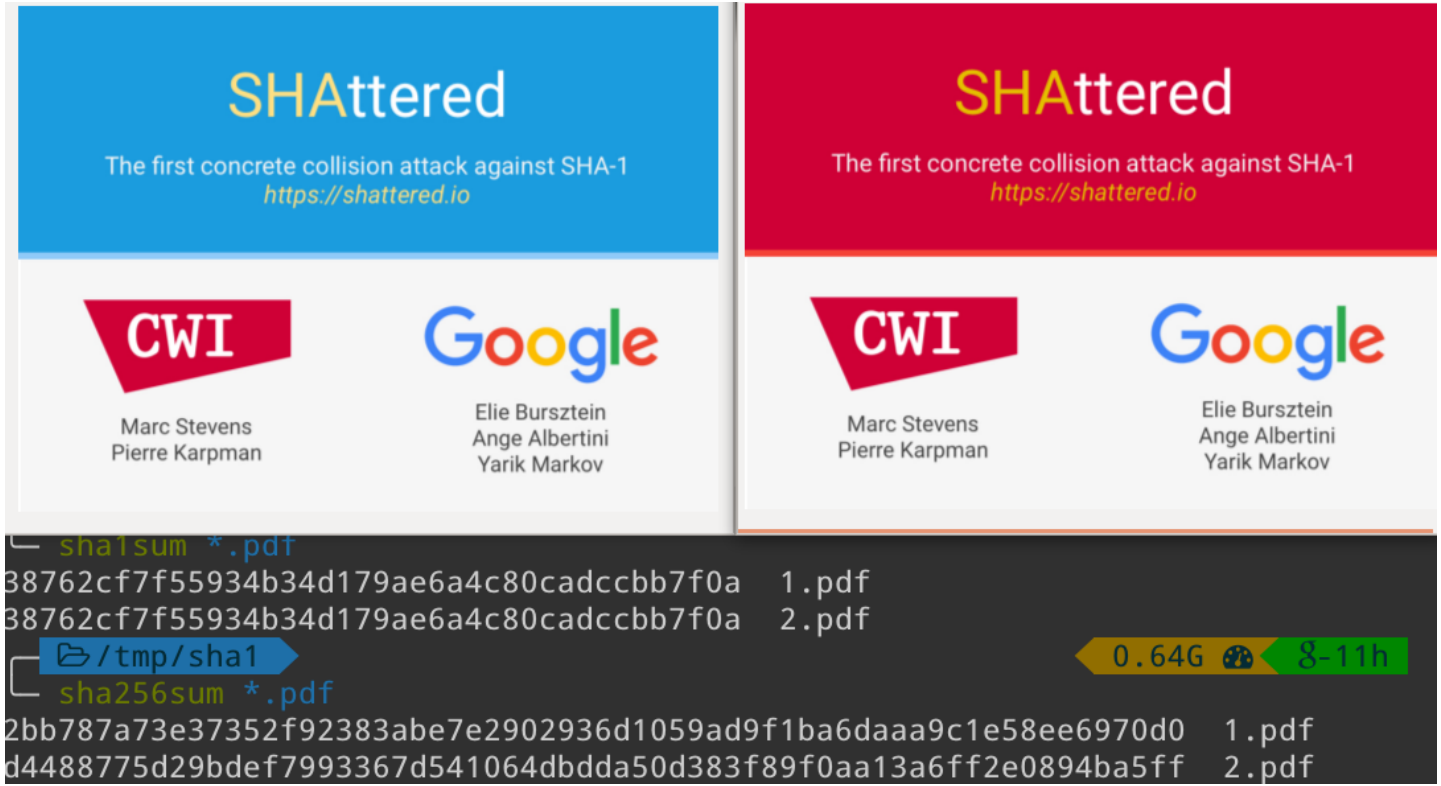


Ref: https://xkcd.com/538/

Cryptography

- Hash collisions
  - Because hashes have a fixed length output, it is mathematically possible for 2 inputs to produce the same output.
    A good hashing algorithm makes this extremely hard to do.
  - MD5 had a weakness found in 1996, and a collision attack published in 2004
  - SHA-1 had theoretical attacks published in 2005, and the NIST officially deprecated SHA-1 in 2011

Cryptography



Ref: https://shattered.io/

Any Questions?