Cryptology = Cryptography + Cryptanalysis

The National Security Agency (NSA): a national-level intelligence agency of the US Dept of Defense, which is responsible for global monitoring, collection, and processing of information and data for foreign intelligence and counterintelligence purposes, specializing in a discipline known as signals intelligence (SIGINT).

The National Institute of Standards and Technology(NIST): a measurement standards laboratory, and a non-regulatory agency of the US Dept of Commerce, whose mission is to promote innovation and industrial competitiveness.

Cryptography backdoor: a method, often secret, of bypassing normal encryption in a cryptosystem. It allows an intruder to access the plaintext without having the correct user credentials.

Key escrow: an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys.

Decryption order: an order that forces suspects to decrypt their encrypted data or give up their keys.

Whitfield Diffie: one of the pioneers of public-key cryptography; co-inventor of Diffie-Hellman key exchange; won the 2015 Turing Award.

Ron Rivest: co-inventor of the RSA algorithm; inventor of the symmetric-key encryption algorithms RC2/RC4/RC5; inventor of the MD2/MD4/MD5/MD6 cryptographic hash functions; co-author of \Introduction to Algorithms" book; won the 2002 Turing Award.

Alice, Bob, Eve, Mallory: Check https://en.wikipedia.org/wiki/Alice_and_Bob#Cast_of_characters.

Trent (or Ted): a trusted arbitrator as a neutral third party.

Graphical passwords: A graphical password or graphical user authentication is a form of authentication using images rather than letters, digits, or special characters. The type of images used and the ways in which users interact with them vary between implementations.

Covert channel: In computer security, a covert channel is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.

Side Channel Attack: In computer security, a side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited.

Notice that a covert channel is a channel intentionally created by an attacker to leak information out of the target system; whereas a side channel is an unintentional channel taken advantage by an attacker to obtain more information about the target system. A side channel attack exploits a side channel.

End-to-end encryption: End-to-end encryption (E2EE) is a system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers – including telecom providers, Internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation
End-to-end encryption is intended to prevent data being read or secretly modified, other than by the true sender and recipient(s). The messages are encrypted by the sender but the third party does not have a means to decrypt them, and stores them encrypted. The recipients retrieve the encrypted data and decrypt it themselves.
Because no third parties can decipher the data being communicated or stored, for example, companies that provide end-to-end encryption are unable to hand over texts of their customers' messages to the authorities.

Single Sign On (SSO): Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. True single sign-on allows the user to log in once and access services without re-entering authentication factors.

Hardware RNG: In computing, a hardware random number generator (HRNG) or true random number generator (TRNG) is a device that generates random numbers from a physical process, rather than by means of an algorithm. Such devices are often based on microscopic phenomena that generate low-level, statistically random "noise" signals, such as thermal noise, the photoelectric effect, involving a beam splitter, and other quantum phenomena. These stochastic processes are, in theory, completely unpredictable for as long as an equation governing such phenomena is unknown or uncomputable, and the theory's assertions of unpredictability are subject to experimental test. This is in contrast to the paradigm of pseudo-random number generation commonly implemented in computer programs.

Quantum RNG: Quantum RNGs exploit elementary quantum optic processes that are fundamentally probabilistic to produce true randomness. As the quantum processes underlying the QRNG are well understood and characterized, their inner workings can be clearly modelized and controlled to always produce unpredictable randomness.

Retinal vs Iris Scan: Retina scans are 70x more accurate than iris scans. Iris scans capture an image of the iris from a distance, while retina scanning does it by placing the person's eye near to an eyepiece. Retina scanning is best suited for physical identification

Be aware of the differences between pseudo random number generators and hardware random number generators by reading, for instance https://en.wikipedia.org/wiki/List_of_random_number_generators.

Nonce: In cryptography, a nonce (number once) is an arbitrary number that can be used just once in a cryptographic communication. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks. They can also be useful as initialization vectors and in cryptographic hash functions.

Encryption

Correctness m = Dk(Ek(m))
Efficiency encrypt, decrypt, generate key must be fast
Security difficult to recover secret key or plaintext
Computational security => 2^128 keys

Attacks on Cipher

ciphertext only – a large number of ciphertexts all encrypted using the same key
known plaintext – pairs of ciphertext and the corresponding plaintext

Substitution Cipher

Substitution table representing 1-1 mapping from U to U
Monoalphabetic (1-1 mapping/ substitution fixed for each alphabet)
Key space => set of all possible keys
Key space size = |U|! E.g 27! For alphabet + '_'
Key size => minimum number of bits to represent all possible keys
Key size = log2(key space size) e.g log2(27!) = 94 bits = log(27!)/log(2)

Encryption = mapping, Decryption = inverse

Known plaintext

1. Brute force => check all possible keys to find key where Ek(X) = C
    a. (27!) loops/operations
2. Determine key given plaintext and ciphertext just by matching
    a. Sufficiently enough or long ciphertext/plaintext pair can determine full table

Insecure under known plaintext because of 2.
Ciphertext only

3. Brute force => check all possible keys to find key where Dk(C) = english/semantic
    a. (27!) loops/operations
    b. Small probability wrong key
4. Frequency analysis on monoalphabetic cipher
    a. Compare frequency with letter frequency distribution

Insecure under known ciphertext because of 4.

Shift/Caesar Cipher

Each letter in plaintext shifted down fixed number of places e.g rot13
Monoalphabetic
Key space size = |U| e.g 27 (alphabet + '_')
Key size = log2(|U|)

Easy to break with brute force
Same attacks as Substitution (subset of substitution ciphers)

Vignere Cipher

Shift by keyword(string of letters representing numbers based on position in alphabet)
Keyword repeated for longer plaintext
Polyalphabetic (each character shift based on current index of keyword)
Same character can be mapped to different characters

Each character of keyword has 27 choices (alphabet + space/underscore)
Key space size = 27^|length of key|
Key size = log2(27^|length of key|)

Vignere > substitution
27^x > 27!
Length of keyword at least 20

Insecure under known plaintext => determine key by distance of each plaintext character and ciphertext character, key repeats for longer plaintext

Insecure against ciphertext only given we can determine length/period of keyword
All letters whose index is i(mod k) gets shifter by same character in keyword (monoalphabetic)
Frequency analysis on each group shifted by same key

Determine period of keyword with kasiski method, repeated patterns

Permutation Cipher

Permutation to each block
Key space size = |length of block|!
Key size = log2(|length of block|!)

Insecure under known plaintext, just match
Insecure under ciphertext only if plaintext in English

One time Pad

Key as long as plaintext
Encrypt => plaintext XOR key to get ciphertext
Decrypt => ciphertext XOR key to get plaintext

Insecure under known plaintext but key will not be reused
One time pad leaks no information of plaintext except length
Perfect secrecy/unbreakable

If key k is random, ciphertext c looks as random as key

If k[0] = 0, X[0] = C[0]
If k[0] = 1, X[0] = C[0]'

Both probability = ½

Fails with repeated key
Key must be as long as plaintext

Attacker Capabilities (weakest to strongest)

Ciphertext only same key
Known plaintext => can observe ciphertext and know corresponding plaintext, same key
Chosen plaintext => can encrypt plaintext of choice, same key
Chosen ciphertext => can decrypt ciphertext of choice + encrypt plaintext, same key

Side channel attack => exploit source of info that depends on implementation of cipher
Observe/measure analog characteristics but cannot alter integrity
E.g execution time, power, noise

Invasive attack => can alter integrity

Modern Cipher

Block cipher high diffusion => change to key/plaintext spread across ciphertext
Stream cipher low diffusion

Confusion => complex transformation, unable to predict change

Substitution => confusion
Permutation => diffusion

Sniffing is the process in which all the data packets passing in the network are monitored. ... Sniffers can be hardware or software installed on the system. Spoofing is the process in which an intruder introduces fake traffic and pretends to be someone else

Boiled down: phishing aims to take hold of personal information by convincing the user to provide it directly; spoofing aims to steal or disguise an identity so malicious activity can ensue. Both employ a level of disguise and misrepresentation, so it is easy to see why they are so closely paired.

Skimming in cybersecurity refers to cybercriminals' strategies for capturing and stealing cardholder's personal payment information. Identity thieves use various approaches to obtain card data. One of the most advanced methods is using a small skimming device designed to read a credit card's microchip or magnetic strip information. Criminals can execute skimming attacks whenever a cardholder opts for electronic payment methods in a physical location.

Skimming => card reader + camera for PIN

False Match Rate = successful false match/all false attempts = fake but get in

False Non Match Rate = rejected genuine attempt /all genuine = real but rejected

Increase Threshold = stricter = reduce FMR = increase FNMR

0 Threshold = anyone can get in
1 Threshold = nobody can get in

Failure to enroll => cannot register biometrics
Failure to capture => fail to capture during authentication

2FA => 2 factors for authentication

E.g password, OTP, biometrics

SMS OTP can be intercepted if message not end to end encrypted

Not 1 way => not collision resistant

Collision resistant => 1 way

If h(F) = h(F') , very high confidence F = F' since collision resistant

Work factor on breaking cipher is M to find collision with high probability

$M > 1.17T^{0.5}$

Digest length must be higher than key length

PKI = Certificate + CA + trust hierarchy + certificate revocation

Typosquatting => just wait for people to click spoofed link