Security Models and Concepts

Security architecture frameworks	
Zachman Framework	A 2D model considering interrogations such as what, where and when with, etc. With various views such as planner, owner, designer etc.
Sherwood Applied Business Security Architecture (SABSA)	To facilitate communication between stakeholders
Information Technology Infrastructure Library (ITIL)	Set of best practices for IT service management
Security architecture documentation	
ISO/IEC 27000 Series	Establish security controls published by Standardization (ISO) and the Electrotechnical Commission (IEC)
Control Objectives for Information and Related Technology (CobiT)	Define goals and requirements for security controls and the mapping of IT security controls to business objectives.
Types of security models	
State Machine Models	Check each of the possible system state and ensure the proper security relationship between objects and subjects in each state.
Multilevel Lattice Models	Allocate each security subject a security label defining the highest and lowest boundaries of the subject's access to the system. Enforce controls to all objects by dividing them into levels known as lattices.
Matrix Based Models	Arrange tables known as matrix which includes subjects and objects defining what actions subjects can take upon another object.
Noninterference Models	Consider the state of the system at a point in time for a subject, it consider preventing the actions that take place at one level which can alter the state of another level.
Information Flow Models	Try to avoid the flow of information from one entity to another which can violate the security policy.
Confinement	Read and Write are allowed or restricted using a specific memory location, e.g. Sandboxing.
Data in Use	Scoping & tailoring

Security Modes

Dedicated Security Mode	Use a single classification level. All objects can access all subjects, but users they must sign an NDA and approved prior to access on need-to-know basis
System High Security Mode	All users get the same access level but all of them do not get the need-to-know clearance for all the information in the system.
Compartmented Security Mode	In addition to system high security level all the users should have need-to-know clearance and an NDA, and formal approval for all access required information.
Multilevel Security Mode	Use two classification levels as System Evaluation and Assurance Levels

Virtualization

Guest operating systems run on virtual machines and hypervisors run on one or more host physical machines.

Virtualization security threats	Trojan infected VMs, misconfigured hypervisor
Cloud computing models	Software as A Service (SaaS), Infrastructure As A Service (IaaS), Platform As A Service (PaaS)
Cloud computing threats	Account hijack, malware infections, data breach, loss of data and integrity

Memory Protection

Register	Directly access inbuilt CPU memory to access CPU and ALU.
Stack Memory Segment	Used by processors for intercommunication.
Monolithic Operating System Architecture	All of the code working in kernel mode/system.
Memory Addressing	Identification of memory locations by the processor.
Register Addressing	CPU access registry to get information.
Immediate Addressing	Part of an instruction during information supply to CPU.
Direct Addressing	Actual address of the memory location is used by CPU.
Indirect Addressing	Same as direct addressing but not the actual memory location.
Base + Offset Addressing	Value stored in registry is used as based value by the CPU.

*Citation CISSP SUMMARY BY Maarten De Frankrijker

Cryptographic Terminology

Encryption	Convert data from plaintext to cipher text.
Decryption	Convert from ciphertext to plaintext.
Key	A value used in encryption conversion process.
Synchronous	Encryption or decryption happens simultaneously.
Asynchronous	Encryption or decryption requests done subsequently or after a waiting period.
Symmetric	Single private key use for encryption and decryption.
Asymmetrical	Key pair use for encrypting and decrypting. (One private and one public key)
Digital Signature	Use to verify authentication and message integrity of the sender. The message use as an input to a hash functions for validating user authentication.
Hash	A one-way function, convert message to a hash value used to verify message integrity by comparing sender and receiver values.
Digital Certificate	An electronic document that authenticate certification owner.
Plaintext	Simple text message.
Ciphertext	Normal text converted to special format where it is unreadable without reconversion using keys.
Cryptosystem	The set of components used for encryption. Includes algorithm, key and key management functions.
Cryptanalysis	Breaking decrypting ciphertext without knowledge of cryptosystem used.
Cryptographic Algorithm	Procedure of enciphers plaintext and deciphers cipher text.
Cryptography	The science of hiding the communication messages from unauthorized recipients.
Cryptology	Cryptography + Cryptanalysis
Decipher	Convert the message as readable.
Encipher	Convert the message as unreadable or meaningless.
One-time pad (OTP)	Encipher all of the characters with separate unique keys.
Key Clustering	Different encryption keys generate the same plaintext message.
Key Space	Every possible key value for a specific algorithm.
Algorithm	A mathematical function used in encryption and decryption of data; A.K.A. cipher.
Cryptology	The science of encryption.
Transposition	Rearranging the plaintext to hide the original message; A.K.A. Permutation.
Substitution	Exchanging or repeating characters (1 byte) in a message with another message.
Vernam	Key of a random set of non-repeating characters. A.K.A. One time pad.
Confusion	Changing a key value during each circle of the encryption.
Diffusion	Changing the location of the plaintext inside the cipher text.
Avalanche Effect	When any change in the key or plaintext significantly change the ciphertext.
Split Knowledge	Segregation of Duties and Dual Control.
Work factor	The time and resources needed to break the encryption.
Nonce	Arbitrary number to provide randomness to cryptographic function.
Block Cipher	Dividing plaintext into blocks and assign similar encryption algorithm and key.
Stream Cipher	Encrypt bit wise - one bit at a time with corresponding digit of the keystream.
Dumpster Diving	Unauthorized access a trash to find confidential information.
Phishing	Sending spoofed messages as originate from a trusted source.
Social Engineering	Mislead a person to provide confidential information.
Script kiddie	A moderate level hacker that uses readily found code from the internet.

Requirements for Hashing Message Digest

Variable length input - easy to compute - one way function - digital signatures - fixed length output

MD Hash Algorithms

MD2	128-bit hash, 18 rounds of computations
MD4	128-bit hash. 3 rounds of computations, 512 bits block sizes
MD5	128-bit hash. 4 rounds of computations, 512 bits block sizes, Merkle–Damgård construction
MD6	Variable, 0<d≤512 bits, Merkle tree structure
SHA-0	Phased out, collision found with a complexity of 2^33.6 (approx 1 hr on standard PC) Retired by NIST
SHA-1	160-bit MD, 80 rounds of computations, 512 bits block sizes, Merkle–Damgård construction (not considered safe against well funded attackers)
SHA-2	224, 256, 384, or 512 bits, 64 or 80 rounds of computations, 512 or 1024 bits block sizes, Merkle–Damgård construction with Davies–Meyer compression function

Security Models

MATRIX (Access control model)	- Provides access rights including discretionary access control to subjects for different objects. - Read, write and execute access defined in ACL as matrix columns and rows as capability lists.
BELL-LAPADULA (Confidentiality model)	-A subject cannot read data at a higher security level. (A.K.A simple security rule) - Subject in a defined security level cannot write to a lower security level unless it is a trusted subject. (A.K.A *-property (star property) rule - Access matrix specifies discretionary access control. - subject with read and write access should write and read at the same security level (A.K.A Strong star rule :) - Tranquility prevents security level of subjects change between levels.
BIBA (Integrity model)	- Cannot read data from a lower integrity level (A.K.A The simple integrity axiom) - Cannot write data to an object at a higher integrity level. (A.K.A the * (star) integrity axiom) - Cannot invoke service at higher integrity. (A.K.A The invocation property) - Consider preventing information flow from a low security level to a high security level.
CLARK WILSON (Integrity model)	User: An active agent • Transformation Procedure (TP): An abstract operation, such as read, writes, and modify, implemented through Programming • Constrained Data Item (CDI): An item that can be manipulated only through a TP • Unconstrained Data Item (UDI): An item that can be manipulated by a user via read and write operations - Enforces separation of duty - Requires auditing - Commercial use - Data item whose integrity need to be preserved should be audited - An integrity verification procedure (IVP) -scans data items and confirms their integrity against external threats
Information flow model	Information is restricted to flow in the directions that are permitted by the security policy. Thus flow of information from one security level to another. (Bell & Biba).
Brewer and Nash (A.K.A Chinese wall model)	- Use a dynamic access control based on objects previous actions. - Subject can write to an object if, and only if, the subject cannot read another object in a different dataset. - Prevents conflict of interests among objects. Citation https://ipspecialist.net/fundamental-concepts-of-security-models-how-they-work/
Lipner Model	Commercial mode (Confidentiality and Integrity,) -BLP + Biba
Graham-Denning Model Objects, subjects and 8 rules	Rule 1: Transfer Access, Rule 2: Grant Access, Rule 3: Delete Access, Rule 4: Read Object, Rule 5: Create Object, Rule 6: destroy Object, Rule 7: Create Subject, Rule 8: Destroy
Harrison-Ruzzo-Ullman Model	Restricts operations able to perform on an object to a defined set to preserve integrity.

Web Security

OWASP	Open-source application security project. OWASP creates guidelines, testing procedures, and tools to use with web security.
OWASP Top 10	Injection / SQL Injection, Broken Authentication, Sensitive Data Exposure, XML External Entity, Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging and Monitoring
SQL Injections:	Attackers try to exploit by allowing user input to modify the back-end/server of the web application or execute harmful code which includes special characters inside SQL codes results in deleting database tables etc.
SQL Injection prevention:	Validate the inputs and parameters.
Cross-Site Scripting (XSS)	Attacks carryout by inputting invalidated scripts inside webpages.
Cross-Request Forgery	Attackers use POST/GET requests of the http web pages with HTML forms to carry out malicious activity with user accounts. Prevention can be done by authorization user accounts to carry the actions. Eg. using a Random string in the form, and store it on the server.

Cryptography

Cryptography Goals (P.A.I.N.)	• P - Privacy (Confidentiality) • A – Authentication • I - Integrity • N - Non-Repudiation. • Key space = 2n. (n is number of key bits)
Use of Cryptography	• Confidentiality • Integrity • Proof of origin • Non-repudiation • Protect data at rest • Protect data in transit

Codes vs. Ciphers

Classical Ciphers	Substitution cipher, Transposition cipher, Caesar Cipher, Concealment.
Modern Ciphers	Block cipher, Stream cipher, Steganography, Combination.
Concealment Cipher	Cipher converts Plaintext to another written text to hide original text.
Substitution Ciphers	Uses a key to substitute letters or blocks of letters with different letters or block of letters. I.e. One-time pad, stenography.
Transposition Ciphers	Reorder or scramble the letters of the original message where the key used to decide the positions to which the letters are moved.

Common Algorithms

Algorithm	Symmetric/ Asymmetric	Key length	Based on	Structure
DES	Symmetric	64 bit	128-bit Lucifer algorithm	64 bit cipher block size and 56 bit key with 8 bits parity. • 16 rounds of transposition and substitution (ECB, CBC, CFB, OFB, CTR)
3 DES or TDES (Triple DES)	Symmetric	56 bit*3	DES	3 * 56 bit keys • Slower than DES but higher security (DES EE3, DES EDE3 ,DES EEE2, DES EDE2)
AES	Symmetric	128,192 or 256 bit	Rijndael algorithm	Use 3 different bit size keys Examples Bitlocker, Microsoft EFS Fast, secure 10,12, and 14 transformation rounds
IDEA	symmetric	128 bit		64 bit cipher blocks each block divide to 16 smaller blocks Each block undergo 8 rounds of transformation Example PGP
Skipjack	Symmetric	80 bit		64 bit Block cipher
Blowfish	Symmetric	32-448bit		64 bit Block cipher
TwoFish	Symmetric	128, 192, 256		128 bit blocks
RC4	Symmetric	40-2048		Example SSL and WEP • Stream cipher • 256 Rounds of transformation
RC5	Symmetric	2048		255 rounds transformation • 32, 64 & 128 bit block sizes
CAST	Symmetric	CAST 128 (40 to 128 bit) CAST 256 (128 to 256 bit)		64 bit block 12 transformation rounds 128 bit block 48 rounds transformation
Diffie - Hellman	Asymmetric			No confidentiality, authentication, or non-repudiation • Secure key transfer
RSA	Asymmetric	4096 bit		Uses 1024 keys • Public key and one-way function for encryption and digital signature verification • Private key and one-way function for decryption and digital signature generation • Used for encryption, key exchange and digital signatures
Elgamal	Asymmetric	Any key size	Diffie - Hellman algorithm	Used for encryption, key exchange and digital signatures • Slower
Elliptic Curve Cryptosystem (ECC)	Asymmetric	Any key size		Used for encryption, key exchange and digital signatures • Speed and efficiency and better security

System Evaluation and Assurance Levels

Trusted Computer System Evaluation Criteria (TCSEC)	Evaluates operating systems, application and systems. But not network part. Consider only about confidentiality. Operational assurance requirements for TCSEC are: System Architecture, System Integrity, Covert Channel analysis, Trusted Facility Management and Trusted recovery.
Orange Book	A collection of criteria based on the Bell-LaPadula model used to grade or rate the security offered by a computer system product.
Red Book	Similar to the Orange Book but addresses network security.
Green Book	Password Management.
Trusted Computer System Evaluation Criteria (TCSEC)	Evaluates operating systems, application and systems. But not network part. Consider only about confidentiality. Operational assurance requirements for TCSEC are: System Architecture, System Integrity, Covert Channel analysis, Trusted Facility Management and Trusted recovery.
ITSEC	Consider all 3 CIA (integrity and availability as well as confidentiality

TCSEC	Explanation
D	Minimal protection
C1	DAC; Discretionary Protection (identification, authentication, resource protection)
C2	DAC; Controlled access protection
B1	MAC; Labeled security (process isolation, devices)
B2	MAC; Structured protection
B3	MAC; security domain
A	MAC; verified protection

Common criteria assurance levels

EAL0	Inadequate assurance
EAL1	Functionality tested
EAL2	Structurally tested
EAL3	Methodically tested and checked
EAL4	Methodically designed, tested and reviewed
EAL5	Semi-formally designed and tested
EAL6	Semi-formally verified, designed and tested
EAL7	Formally verified, designed and tested

ITSEC security evaluation criteria - required levels

D + E0	Minimum Protection
C1 + E1	Discretionary Protection (DAC)
C2 + E2	Controlled Access Protection (Media cleansing for reusability)
B1 + E3	Labelled Security (Labelling of data)
B2 + E4	Structured Domain (Addresses Covert channel)
B3 + E5	Security Domain (Isolation)
A + E6	Verified Protection (B3 + Dev Cycle)

Common criteria protection profile components

Descriptive Elements • Rationale • Functional Requirements • Development assurance requirements • Evaluation assurance requirements

Certification & Accreditation

Certification	Evaluation of security and technical/non-technical features to ensure if it meets specified requirements to achieve accreditation.
Accreditation	Declare that an IT system is approved to operate in predefined conditions defined as a set of safety measures at given risk level.

NIACAP Accreditation Process

Phase 1: Definition • Phase 2: Verification • Phase 3: Validation • Phase 4: Post Accreditation

Accreditation Types

Type Accreditation	Evaluates a system distributed in different locations.
System Accreditation	Evaluates an application system.
Site Accreditation	Evaluates the system at a specific location.

Symmetric vs. Asymmetric Encryption

Symmetric Algorithms	Use a private key which is a secret key between two parties. Each party needs a unique and separate private key. Number of keys = x(x-1)/2 where x is the number of users. Eg. DES, AES, IDEA, Skipjack, Blowfish, Twofish, RC4/5/6, and CAST.
Stream Based Symmetric Cipher	Encryption done bitwise and use keystream generators Eg. RC4.
Block Symmetric Cipher	Encryption done by dividing the message into fixed-length blocks Eg. IDEA, Blowfish and, RC5/6.
Asymmetric Algorithms	Use public and private key where both parties know the public and the private key known by the owner .Public key encrypts the message, and private key decrypts the message. 2x is total number of keys where x is number of users. Eg. Diffie-Hellman, RSA, El Gamal, ECC, Knapsack, DSA, and Zero Knowledge Proof.

Symmetric Algorithms	Asymmetric Algorithms	Hybrid Cryptography
Use of private key which is a secret key	Use of public and private key pairs	Use of both Symmetric and Asymmetric encryption. Eg. SSL/TLS
Provides confidentiality but not authentication or nonrepudiation	Provides confidentiality, integrity, authentication, and nonrepudiation	Provide integrity. One way function divides a message or a data file into a smaller fixed length chunks.
One key encrypts and decrypts	One key encrypts and other key decrypts	Encrypted with the private key of the sender.
Larger key size. Bulk encryptions	Small blocks and key sizes	Message Authentication Code (MAC) used to encrypt the hash function with a symmetric key.
Faster and less complex. Not scalable	Slower. More scalable.	Allows for more trade-offs between speed, complexity, and scalability.
Out-of-band key exchange	In-band key exchange	Hash Functions and Digital Certificates Hashing use message digests.

Key Escrow and Recovery

Secret key is divided into two parts and handover to a third party.

PKI

confidentiality, message integrity, authentication, and nonrepudiation

Receiver's Public Key-Encrypt message
Sender Private Key-Decrypt message
Sender Private Key-Digitally sign
Sender's Public Key - Verify Signature

PKI Structure

Certificates	Provides authorization between the parties verified by CA.
Certificate Authority	Authority performing verification of identities and provides certificates.
Registration Authority	Help CA with verification.
Certification Path Validation	Certificate validity from top level.
Certification Revocation List	Valid certificates list
Online Certificate status protocol (OCSP)	Used to check certificate validity online
Cross-Certification	Create a trust relationship between two CA's

Digital Signatures

- Sender's private key used to encrypt hash value
- Provides authentication, nonrepudiation, and integrity
- Public key cryptography used to generate digital signatures
- Users register public keys with a certification authority (CA).
- Digital signature is generated by the user's public key and validity period according to the certificate issuer and digital signature algorithm identifier.

Digital Certificate - Steps

Enrollment - Verification - Revocation

Cryptography Applications & Secure Protocols

Hardware -BitLocker and truecrypt	• **BitLocker:** Windows full volume encryption feature (Vista onward) • **truecrypt:** freeware utility for on-the-fly encryption (discontinued)
Hardware-Trusted Platform Module (TPM)	A hardware chip installed on a motherboard used to manage Symmetric and asymmetric keys, hashes, and digital certificates. TPM protect passwords, encrypt drives, and manage digital permissions.
Link encryption	Encrypts entire packet components except Data Link Control information.
End to end encryption	Packet routing, headers, and addresses not encrypted.
Email (PGP)	Privacy (Encrypt), Authentication (Digital signature), Integrity, (Hash) and Non-repudiation (Digital signature) Email (Secure MIME (S/MIME): Encryption for confidentiality, Hashing for integrity, Public key certificates for authentication, and Message Digests for nonrepudiation.
Web application	SSL/TLS. SSL encryption, authentication and integrity.
Cross-Certification	Create a trust relationship between two CA's
IPSEC	(Privacy, authentication, Integrity, Non Repudiation). Tunnel mode encrypt whole packet (Secure). Transport mode encrypt payload (Faster)
IPSEC components	Authentication Header (AH): Authentication, Integrity, Non repudiation. Encapsulated Security Payload (ESP): Privacy, Authentication, and Integrity. Security Association (SA): Distinct Identifier of a secure connection.
ISAKMP	Internet Security Association Key Management Protocol Authentication, use to create and manage SA, key generation.
Internet Key Exchange (IKE)	Key exchange used by IPsec .Consists of OAKLEY and Internet Security Association and Key Management Protocol (ISAKMP). IKE use Pre-Shared keys, certificates, and public key authentication.
Wireless encryption	Wired Equivalent Privacy (WEP): 64 & 128 bit encryption. Wi-Fi Protected Access (WPA): Uses TKIP. More secure than WEP WPA2: Uses AES. More secure than WEP and WPA.

Hardware architecture

Multitasking	Simultaneous running of two or more tasks.
Multi programming	Simultaneous running of two or more programs
Multi-processing	CPU consists of more than one processor
Processing Types	
Single State	One security level at a time.
Multi State	Multiple security levels at a time.
Firmware	Software built in to in the ROM.
Base Input Output System (BIOS)	Set of instructions used to load OS by the computer.

Mobile Security

Device Encryption • Remote wiping • Remote lock out • Internal locks (voice, face recognition, pattern, pin, password) • Application installation control • Asset tracking (IMIE) • Mobile Device Management • Removable storage (SD CARD, Micro SD etc.)

IoT & Internet Security

Network Segmentation (Isolation) • Logical Isolation (VLAN) • Physical isolation (Network segments) • Application firewalls • Firmware updates

Physical Security

Internal vs external threat and mitigation	
Natural threats	Hurricanes, tornadoes, earthquakes floods, tsunami, fire, etc
Politically motivated threats	Bombs, terrorist actions, etc
Power/utility supply threats	General infrastructure damage (electricity telecom, water, gas, etc)
Man Made threats	Sabotage, vandalism, fraud, theft
Major sources to check	Liquids, heat, gases, viruses, bacteria, movement: (earthquakes), radiation, etc
Natural threat control measures	
Hurricanes, Tornadoes, Earthquakes	Move or check location, frequency of occurrence, and impact. Allocate budget.
Floods	Raised flooring server rooms and offices to keep computer devices .
Electrical	UPS, Onsite generators
Temperature	Fix temperature sensors inside server rooms , Communications - Redundant internet links, mobile communication links as a back up to cable internet.
Man-Made Threats	
Explosions	Avoid areas where explosions can occur Eg. Mining, Military training etc.
Fire	Minimum 2 hour fire rating for walls, Fire alarms, Fire extinguishers.
Vandalism	Deploy perimeter security, double locks, security camera etc.
Fraud/Theft	Use measures to avoid physical access to critical systems. Eg. Fingerprint scanning for doors.

Site Selection

Physical security goals	Deter Criminal Activity - Delay Intruders - Detect Intruders - Assess Situation - Respond to Intrusion
Site selection issues	Visibility - External Entities - Accessibility - Construction - Internal Compartments
Server room security	• Middle of the building (Middle floor) • Single access door or entry point • Fire detection and suppression systems • Raised flooring • Redundant power supplies • Solid /Unbreakable doors
Fences and Gates	8 feet and taller with razor wire. Remote controlled underground concealed gates.
Perimeter Intrusion Detection Systems	Infrared Sensors - Electromechanical Systems - Acoustical Systems - CCTV - Smart cards - Fingerprint/retina scanning
Lighting Systems	Continuous Lighting - Standby Lighting - Movable Lighting - Emergency Lighting
Media storage	Offsite media storage - redundant backups and storage
Electricity	Faraday Cage to avoid electromagnetic emissions - White noise results in signal interference - Control Zone: Faraday cage + White noise
Static Electricity	Use anti-static spray, mats and wristbands when handling electrical equipment - Monitor and maintain humidity levels.
HVAC control levels	Heat - High Humidity - Low Humidity
HVAC Guidelines	• 100F can damage storage media such as tape drives. • 175 F can cause computer and electrical equipment damage. • 350 F can result in fires due to paper based products. • HVAC: UPS, and surge protectors to prevent electric surcharge. • Noise: Electromagnetic Interference (EMI), Radio Frequency Interference Temperatures, Humidity • Computer Rooms should have 15° C - 23°C temperature and 40 - 60% (Humidity)
Voltage levels control	• Static Voltage • 40v can damage Circuits, 1000v Flickering monitors, 1500v can cause loss of stored data, 2000v can cause System shut down or reboot, 17000 v can cause complete electronic circuit damage.
Equipment safety	Fire proof Safety lockers - Access control for locking mechanisms such as keys and passwords.
Water leakage	Maintain raised floor and proper drainage systems. Use of barriers such as sand bags
Fire safety	Fire retardant materials - Fire suppression - Hot Aisle/Cold Aisle Containment - Fire triangle (Oxygen - Heat - Fuel) - Water, CO2, Halon

Fire extinguishers

Class	Type	Suppression
A	Common combustible	Water , SODA acid
B	Liquid	CO2, HALON, SODA acid
C	Electrical	CO2, HALON
D	Metal	Dry Powder

Water based suppression systems	Wet pipes - Dry Pipe - Deluge
Personnel safety	• HI VIS clothes • Safety garments /Boots • Design and Deploy an Occupant Emergency Plan (OEP)
Internal Security	• Programmable multiple control locks • Electronic Access Control - Digital scanning, Sensors • Door entry cards and badges for staff • Motion Detectors- Infrared, Heat Based, Wave Pattern, Photoelectric, Passive audio motion
Key management	Create, distribute, transmission, storage - Automatic integration to application for key distribution, storage, and handling. Backup keys should be stored secure by designated person only.
Testing	Pilot testing for all the backups and safety systems to check the working condition and to find any faults.

Cryptographic Attacks

Passive Attacks	Use eavesdropping or packet sniffing to find or gain access to information.
Active Attacks	Attacker tries different methods such as message or file modification attempting to break encryption keys, algorithm.
Ciphertext-Only Attack	An attacker uses multiple encrypted texts to find out the key used for encryption.
Known Plaintext Attack	An attacker uses plain text and cipher text to find out the key used for encryption using reverse engineering or brute force encryption.
Chosen Plaintext Attack	An attacker sends a message to another user expecting the user will forward that message as cipher text.
Social Engineering Attack	An attacker attempts to trick users into giving their attacker try to impersonate another user to obtain the cryptographic key used.
Brute Force	Try all possible patterns and combinations to find correct key.
Differential Cryptanalysis	Calculate the execution times and power required by the cryptographic device. A.K.A. Side-Channel attacks
Linear Cryptanalysis	Uses linear approximation
Algebraic Attack	Uses known words to find out the keys
Frequency Analysis	Attacker assumes substitution and transposition ciphers use repeated patterns in ciphertext.
Birthday Attack	Assumes figuring out two messages with the same hash value is easier than message with its own hash value
Dictionary Attacks	Uses all the words in the dictionary to find out correct key
Replay Attacks	Attacker sends the same data repeatedly to trick the receiver.
Analytic Attack	An attacker uses known weaknesses of the algorithm
Statistical Attack	An attacker uses known statistical weaknesses of the algorithm
Factoring Attack	By using the solutions of factoring large numbers in RSA
Reverse Engineering	Use a cryptographic device to decrypt the key