Principles of Cyber Security

Information Security

- According to SANS institute, Information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.
- Information Security is based on the following five pillars
  - Confidentiality – data need to be accessed by authorized users
  - Integrity – tamper proof data
  - Availability – system services to authorized users
  - Authentication – ensures data or documents are intended for genuine users
  - Non Repudiation – Sender / Receiver of a message cannot deny the sending or receiving message.

Assets vs. Threats vs. Vulnerability vs. Risk

- An asset is what we're trying to protect.
- A threat is what we're trying to protect against.
- A vulnerability is a weakness or gap in our protection efforts.
- Risk is the intersection of assets, threats, and vulnerabilities.
- What is mean by compromising the system?

Top Information Security Threats

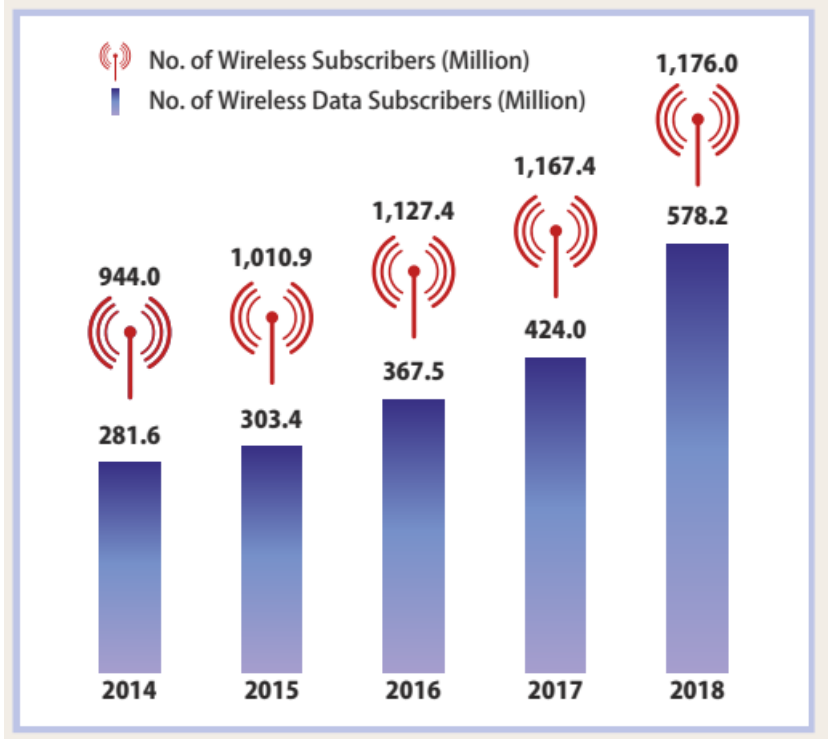
- Insider threats
- Botnets
- Virus and Worms
- Mobile application threats
- Cloud based threats
- IoT Application threats
- Persistent threats

Security Threat Categories

- Network threats
  - Spoofing, sniffing, eavesdropping, ARP poisoning, DNS poisoning, , Denial of Service, Man-in middle, attacks, Password attacks, session hijacking, attacks on Firewall and IDS, and others
- Host threats
  - Physical security threats, Unauthorized access, Password attacks, Footprinting, Malwares, Malicious/Arbitrary code execution, Backdoor attacks, and others.
- Application threats
  - SQL injection attacks, Error and exception handling mismanagement based attacks, Security misconfiguration, Authentication and authorization attacks, cryptography attacks, information disclosure, and others.

Motivation - Internet Usage – A reason for cyber threats

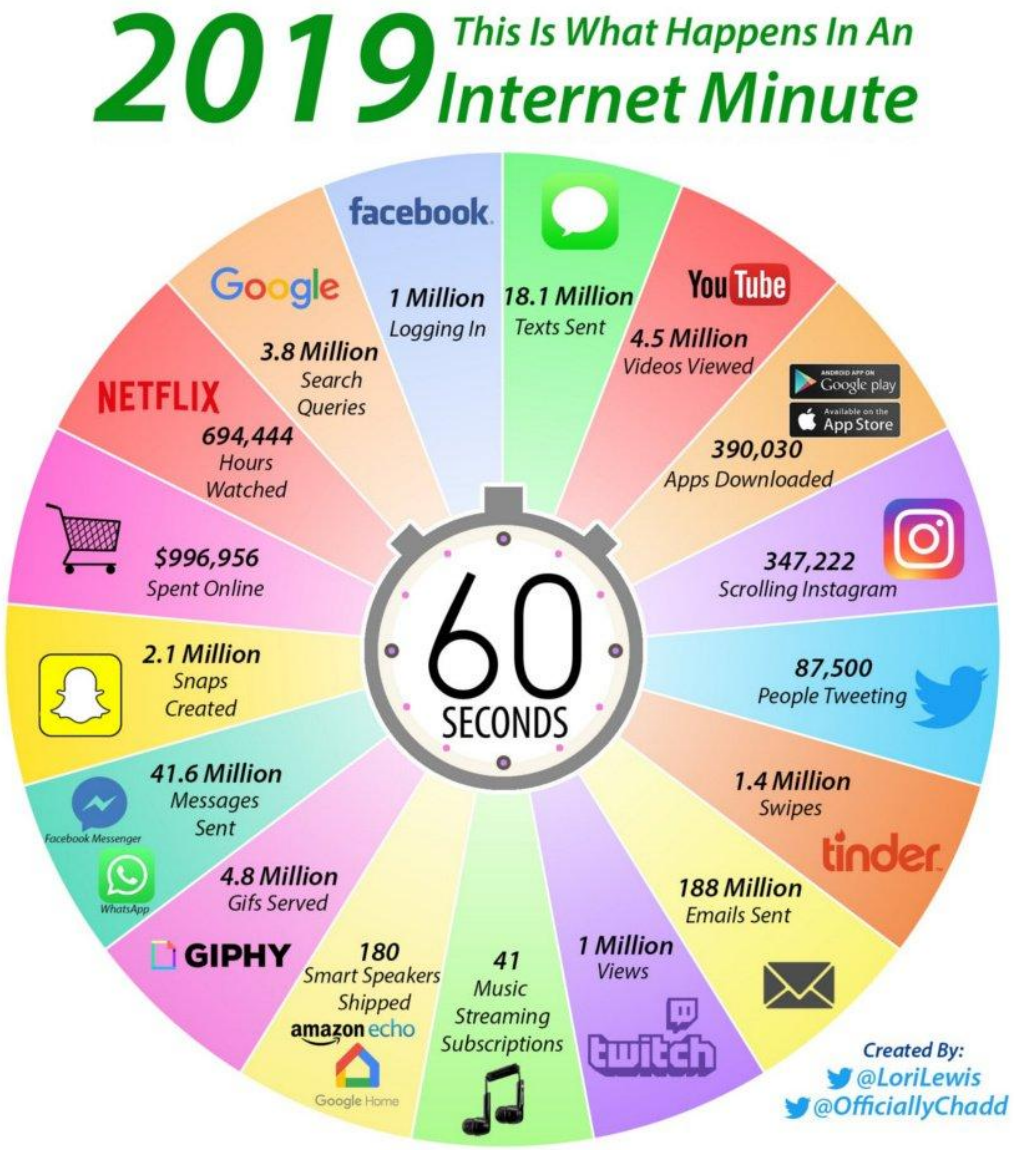
- Around 42 Billion people across the world are using the Internet.
- There is an increase of 7% Internet users from 2018 to 2019.
- In India, the number of Internet users have been increased rapidly from past 5 years.
- According to TRAI, trend of total wireless telephone subscribers and total wireless data subscribers has been significantly increased.
- Central government initiatives such as digital India given a push to use huge number of digital devices with Internet connectivity by the public.



Ref: TRAI 2019 report Govt of India.

Increased Connectivity

- Rapid growth of users in the Social Media Sites.
  - Politicians/Governments are using Social media platforms to reach public.
  - Over 5 million videos are viewed in YouTube for every 60 sec.
  - Over 3 million searches are made in Google for every 60 sec.
  - Many more like this ..
- Rapid growth of online and mobile based payments.
  - In India, use of BHIM app / Phone Pe / Paytm / Google Pay
- Internet data for cheaper cost.



MORE CONNECTIVITY → MORE THREATS

Motivation

- CERT (Computer Emergency Response Team) Govt. Of India, 2019 Report (CERT-In activities during 2019)

Activities	Year 2019
Security Incidents handled	394499
Security Alerts issued	202
Advisories Published	38
Vulnerability Notes Published	204
Trainings Organized	23

Security Incidents	2019
Phishing	472
Unauthorized Network Scanning /Probing/Vulnerable Services	305276
Virus/ Malicious Code	62163
Website Defacements	24366
Website Intrusion & Malware Propagation	417
Others	1805
Total	394499

Recent hacking cases

- The 5 biggest data hacks of 2019
  - https://www.cnbc.com/2019/12/17/the-5-biggest-data-hacks-of-2019.html
- The 15 biggest data breaches of the 21st century
  - https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
- Major Cyber Attacks on India
  - https://www.testbytes.net/blog/cyber-attacks-on-india/
- India was the most cyber-attacked country in the world for three months in 2019
  - https://theprint.in/tech/india-was-the-most-cyber-attacked-country-in-the-world-for-three-months-in-2019/374622/
- Hackers Attack Database of India’s COVID-19 Patients and Potential Suspects
  - https://www.cisomag.com/hackers-attack-database-of-indias-covid-19-patients-and-potential-suspects/

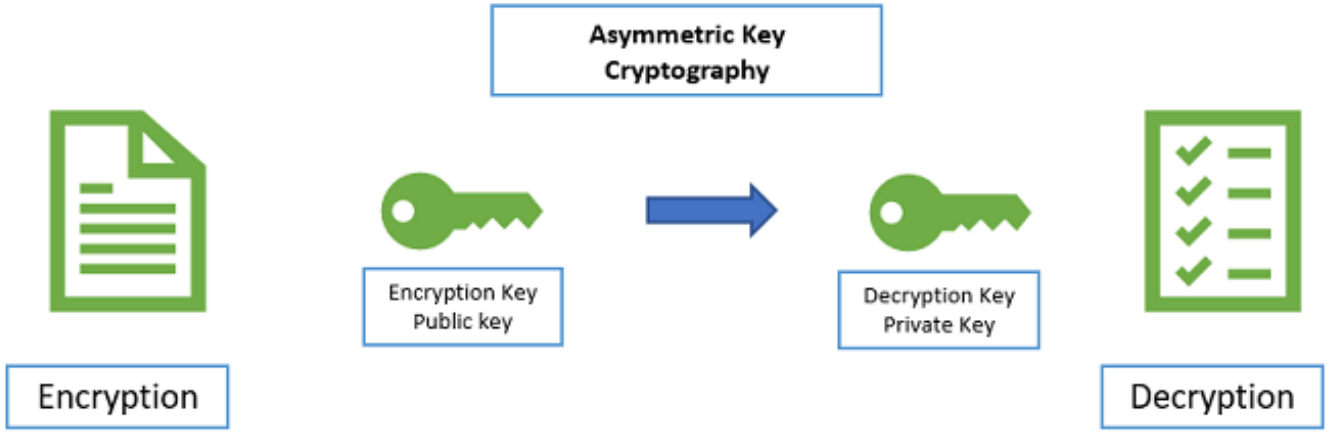
Terms in Cryptography

- Plain Text / Clear Text
- Cipher Text
- Algorithms
- Keys
- Message Digest
- Signature

Symmetric key Algorithms

- Data Encryption Standard (DES) (56-bit key)
- Triple DES (3DES) (168-bit key)
- Blowfish (448-bit key) (optimized for 32-bit and 64-bit architectures)
- International Data Encryption Algorithm (IDEA) (Popular application PGP)
- RC2 (key size vary between 1 and 2048 bits)
- RC4 (key size vary between 1 and 2048 bits) (Ex. WEP)
- RC5 (user can define the key length)
- RC6 (key size vary between 128-256 bits)
- Rijndel or Advanced Encryption Standard (AES) (128/192/256 bit key)
- Twofish (128-256 bit key)

Asymmetric/Public Key Cryptography



Classes of Public Key Algorithms

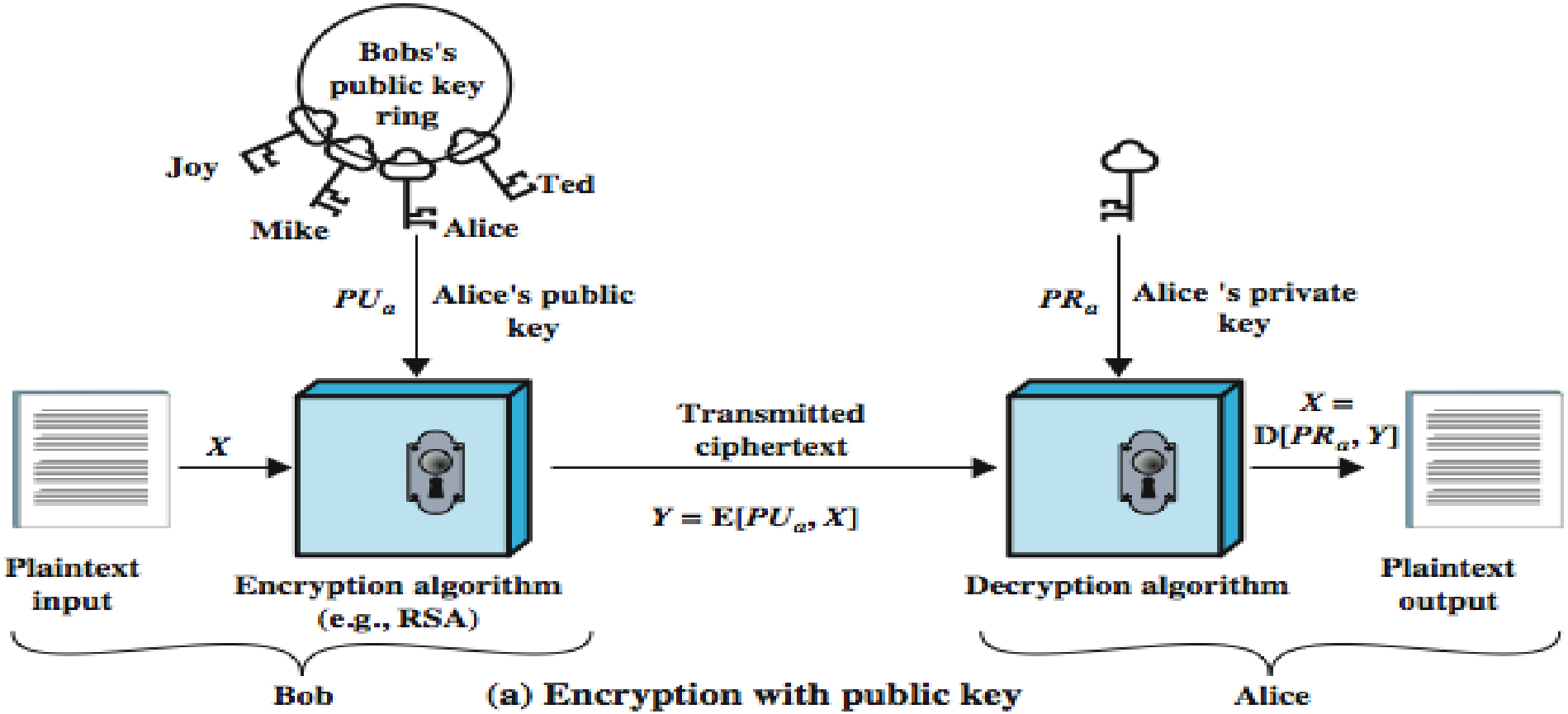
Public Key Distribution Schemes
Public Key Encryption Schemes
Signature Schemes

Every user is supplied with key pair (Pk, Sk). Pk – Public key (Any one can know it) ; Sk – Secrete key
Key pair is unique to each user.
Both keys are used for encryption and decryption.
Two methods: 1) Encryption (Many to One) ; 2) Signature (One to Many)

1) Encryption – Anyone can encrypt msg using Pk. Only intended receiver decrypt using Sk.
2) Signature – Encryption will be done using Sk. Verification will be done by anyone using Pk.

RSA is a very popular public key algorithm in wired networks.

Public-Key Cryptography



Symmetric vs Public-Key

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Public-Key Applications

- can classify uses into 3 categories:
  - **encryption/decryption** (provide secrecy)
  - **digital signatures** (provide authentication)
  - **key exchange** (of session keys)
- some algorithms are suitable for all uses, others are specific to one

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

Security of Public Key Schemes

- like private key schemes brute force **exhaustive search** attack is always theoretically possible
- but keys used are too large (>512bits)
- security relies on a **large enough** difference in difficulty between **easy** (en/decrypt) and **hard** (cryptanalyse) problems
- more generally the **hard** problem is known, but is made hard enough to be impractical to break
- requires the use of **very large numbers**
- hence is **slow** compared to private key schemes

Introduction to Hashing

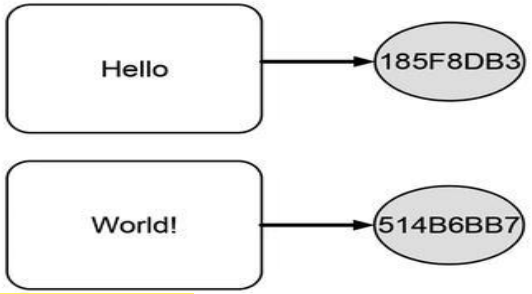
- Hashing in cryptography is used to maintain integrity of data.
- The output of a hash function is also called as digest/ hash value.
- Hash functions takes any length string as input, and outputs a fixed length hash value or digest.
- Hash functions do not require keys to generated hash value.
- Hash value is used to compare the data.

Properties of Hash Functions

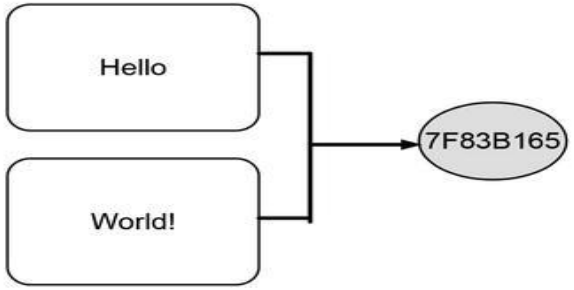
- Pre-Image Resistance
  - This property means that it should be computationally hard to reverse a hash function.
  - In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
  - This property protects against an attacker who only has a hash value and is trying to find the input.
- Second Pre-Image Resistance
  - This property means given an input and its hash, it should be hard to find a different input with the same hash.
  - In other words, if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).
  - This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.
- Collision Resistance
  - This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.
  - In other words, for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y).
  - Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find.
  - This property makes it very difficult for an attacker to find two input values with the same hash.
  - Also, if a hash function is collision-resistant then it is second pre-image resistant.

Hashing the data

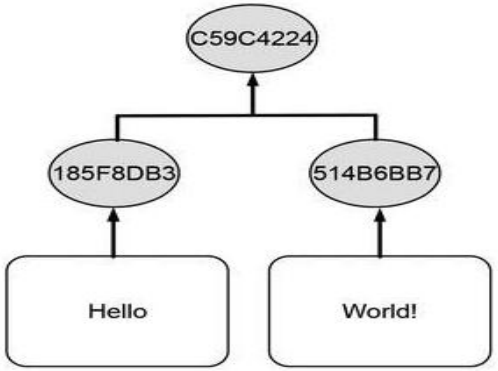
- Independent hashing



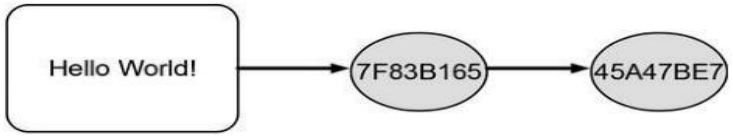
- Combined hashing



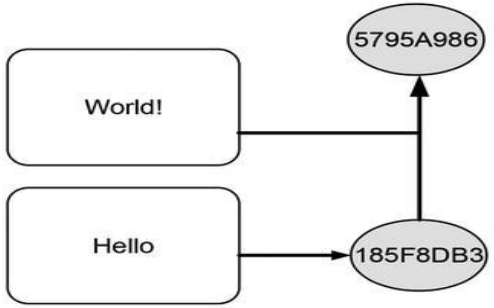
- Hierarchical hashing
  - (Merkle tree)



- Repeated hashing



- Sequential hashing



List of Hashing Algorithms

- Message Digest 2 (MD2)
  - One way hash function used in privacy enhanced mail along with MD5.
- Message Digest 4 (MD4)
  - One way hash function used for PGP
- Message Digest 5 (MD5)
  - Improved version of MD4, produces 128-bit digest.
- Message Digest 6 (MD6)
  - Designed by Ron Rivest
- HAVAL
  - Variable length one way hash function, and modification of MD5
- RIPE-MD
  - Popular hash algorithm across Europe.
- Simple Hash Algorithm – 0 (SHA-0)
  - Basic hash algorithm, later replaced with SHA-1 and SHA-2
- Simple Hash Algorithm – 1 (SHA-1)
  - It has been compromised and replaced by SHA – 2
- Simple Hash Algorithm – 2 (SHA-2)
  - Upgradation to SHA-1 with various hash lengths (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256)

Hashing algorithms comparison

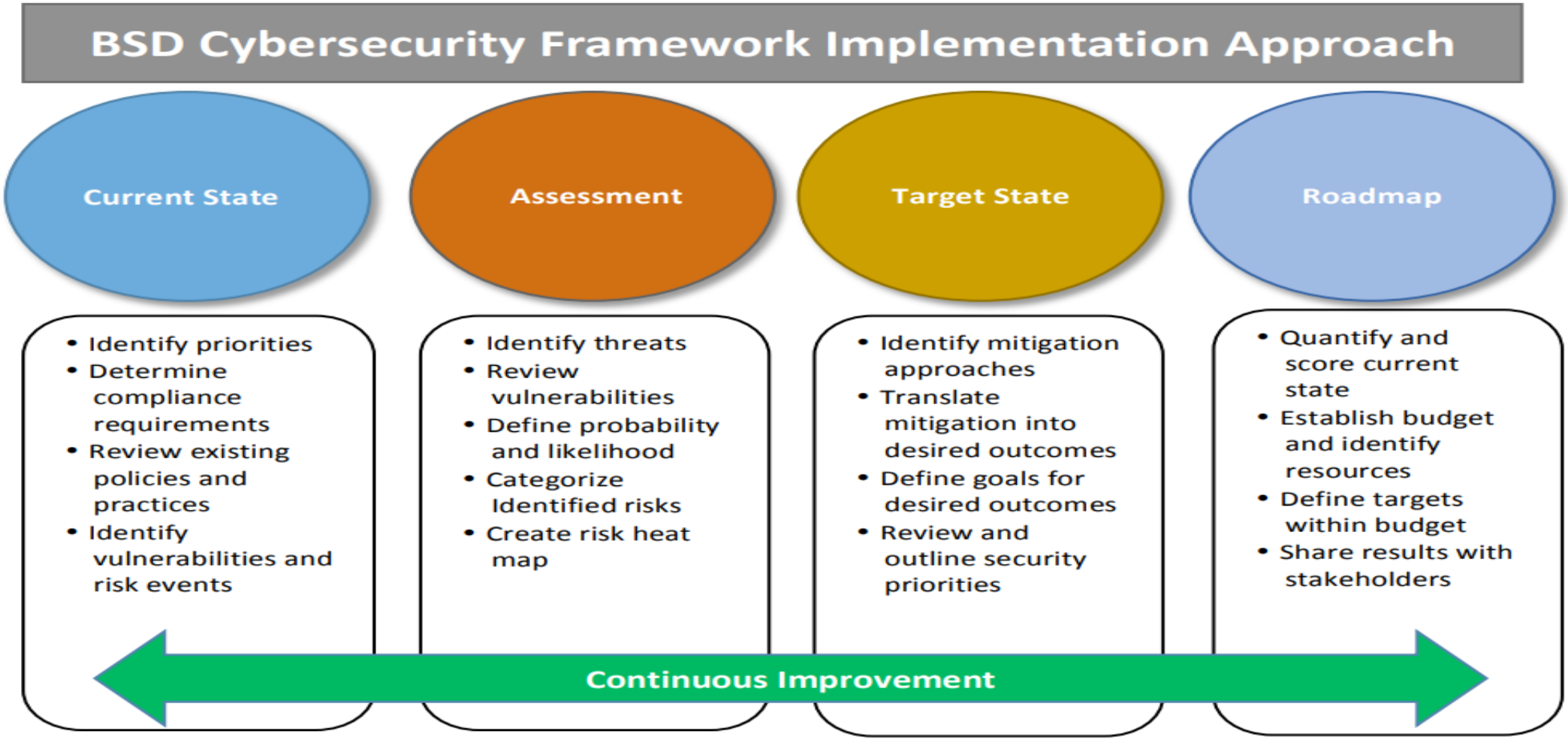
Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Rounds	Operations	Security (bits)	Example performance[2] (MiB/s)
MD5 (as reference)		128	128 (4 × 32)	512	$2^{64} - 1$	64	And, Xor, Rot, Add (mod 2^{32}), Or	<64 (collisions found)	335
SHA-0		160	160 (5 × 32)	512	$2^{64} - 1$	80	And, Xor, Rot, Add (mod 2^{32}), Or	<80 (collisions found)	-
SHA-1		160	160 (5 × 32)	512	$2^{64} - 1$	80		<80 (theoretical attack[3])	192
SHA-2	*SHA-224* *SHA-256*	224 256	256 (8 × 32)	512	$2^{64} - 1$	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112 128	139
	SHA-384 *SHA-512* *SHA-512/224* *SHA-512/256*	384 512 224 256	512 (8 × 64)	1024	$2^{128} - 1$	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192 256 112 128	154
SHA-3	*SHA3-224* *SHA3-256* *SHA3-384* *SHA3-512*	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576	Unlimited[4]	24[5]	And, Xor, Rot, Not	112 128 192 256	-
	SHAKE128 *SHAKE256*	*d* (arbitrary) *d* (arbitrary)		1344 1088				min(*d*/2, 128) min(*d*/2, 256)	-

Cyber Security Principles

- Economy of mechanism
- Fail-safe defaults
- Least Privilege
- Open Design
- Complete mediation
- Separation of Privilege
- Least Common Mechanism
- Psychological acceptability
- Work Factor
- Compromise Recording

Ref: https://www.javatpoint.com/cyber-security-principles

Cyber security Framework (by NIST)



https://www.nist.gov/itl/csd/secure-systems-and-applications

References

1. Computer Security, Principles And Practice by William Stallings Lawrie Brown, Pearson Education
2. Applied Information Security, Dr. David Basin, Springer, 2011
3. Cryptography Theory and Practice (3rd edition), Stinson, Chapman & Hall/CRC
4. Security in Computing (5th edition), Pfleeger, Pfleeger and Margulies, Pearson.
5. Computer Security: Art and Science by Matt Bishop, Addison-Wesley Educational Publishers Inc
6. G. Dileep Kumar, "Network Security Attacks and Countermeasures", IGI Global, 2016.
7. https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
8. https://www.javatpoint.com/cyber-security-principles
9. https://www.youtube.com/watch?v=2zD3etm8D6w
10. https://www.youtube.com/watch?v=5eoWu1ZQF3g