Cryptography

Basics of Cryptography

Malay Bhattacharyya

Assistant Professor

Machine Intelligence Unit
and
Centre for Artificial Intelligence and Machine Learning (CAIML)
Indian Statistical Institute, Kolkata

March 06, 2021

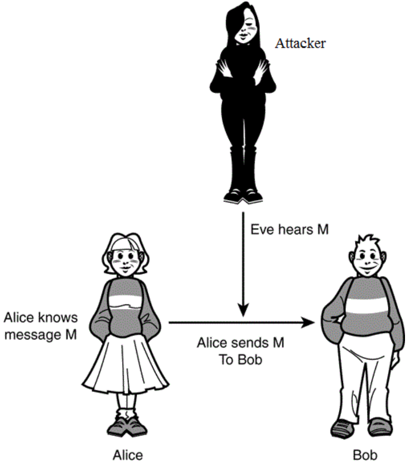
1. Introduction
2. History
3. Basic Terminologies
4. Categories of Attacks
5. Vulnerabilities
6. Suggested Reading

Data and information

Data: Raw or unorganized content (such as alphabets, numbers, or symbols) that refer to, or represent, conditions, ideas, or objects. E.g., 1729, ‘a’, “number”, etc.

Information: A meaningful form of the data. E.g., “1729 is a Ramanujan number”, etc.

How is information attacked?



The message sent by Alice to Bob might be attacked

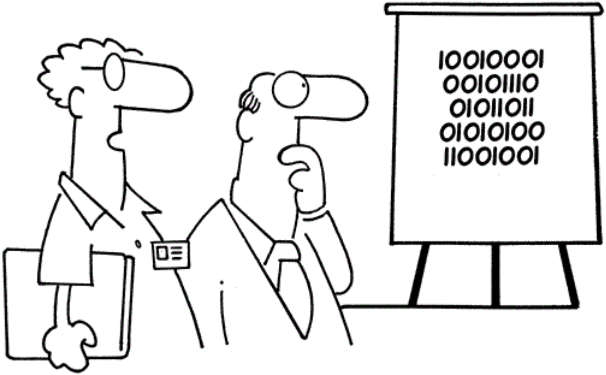
Information security

Information security is the practice of preserving the confidentiality, integrity and availability of information (as outlined in ISO/IEC 27000:2009) from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

- **Confidentiality** ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity** ensures maintaining and assuring the accuracy and completeness of data over its entire life-cycle.
- **Availability** ensures that the information must be available when it is needed.

The art of information security is popularly known as **cryptography**.

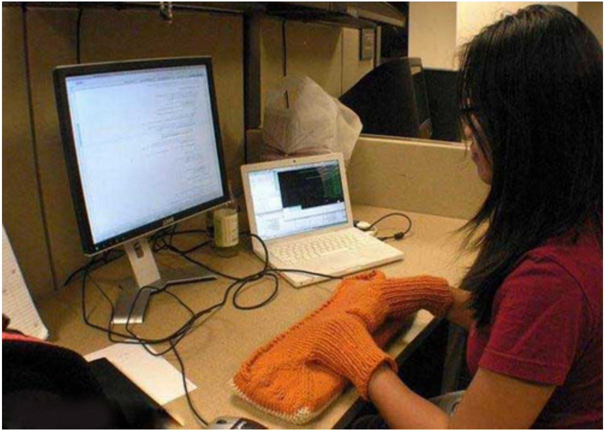
When is your information secure?



"We've devised a new security encryption code.
Each digit is printed upside down."

Clever logic is not always effective

Should we hide ourselves?



Hiding the entry is not a solution of hiding the password

Open (but smart) hiding is important

Logic is known but the key is important

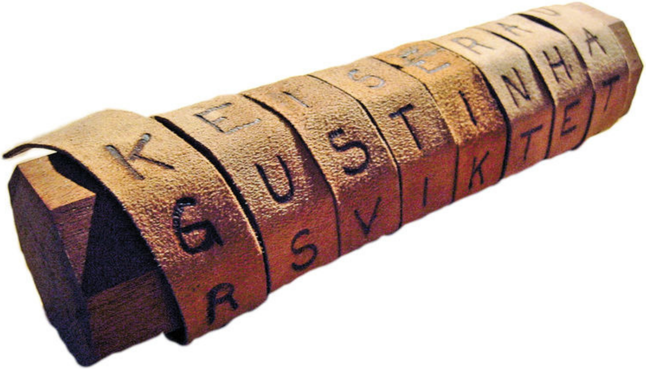
History

"All's fair in love, war, and crypto."

– Anonymous.

650BC: Scytale in the Sparta of Greece
500BC: Use of Atbash ciphers by Hebrew scholars
1942: Use of Enigma machine during WWII
1949: First mathematical theory of cryptography by Claude E. Shannon *The father of modern cryptography*
1975: Data encryption standard (DES) prepared
1977: RSA cryptosystem published
1983: Quantum conjugate coding by S. Wiesner
1990: Quantum key distribution method
2001: Advanced encryption standard (AES) prepared
2012: Keccak algorithm wins SHA-3 hash function competition

The first use of cryptography



Scytale was used by the spartans to send secret message

Notions in cryptography

Definition (Plaintext)

The message to be encoded is known as the plaintext.

Definition (Ciphertext)

Ciphertext is the coded message from plaintext.

Definition (Encryption)

The process of converting from plaintext to ciphertext is known as encryption.

Definition (Decryption)

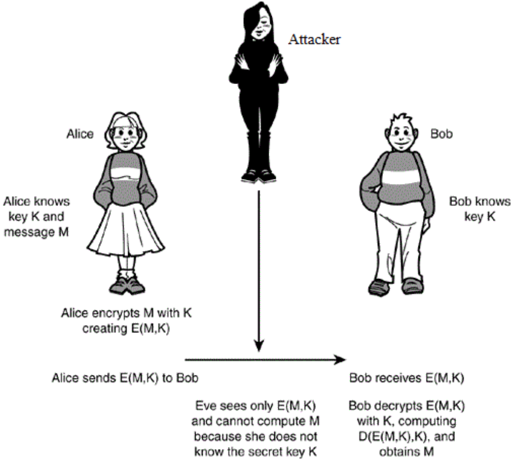
Restoring the plaintext from the ciphertext is known as decryption.

Note: Plaintexts are written in lowercase, ciphertexts in uppercase.

Areas of cryptography

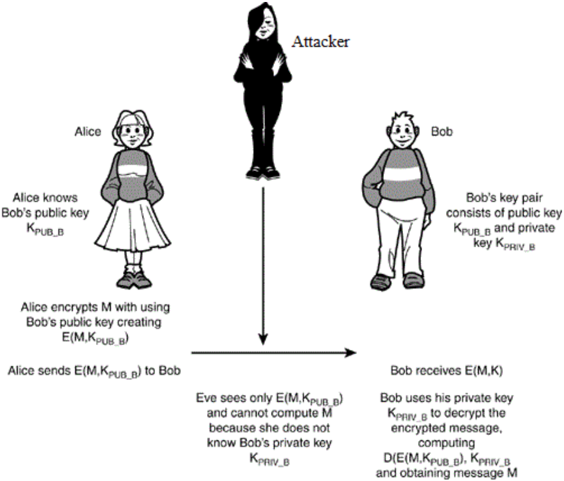
- **Encryption/decryption algorithms:** Concealing the information so that it is not understandable.
  1. **Symmetric:** Alice and Bob both share a single symmetric key. They are the only ones who know the key and no one else is able to read the encrypted message.
  2. **Asymmetric:** Alice and Bob uses two keys – a public and a private one. The public one is available for everyone, but the private one is known only by the owner. When the message is encrypted with the public key, only the corresponding private key can decrypt it. Moreover, the private key can't be learned from the public one.
- **Data integrity algorithms:** Protecting blocks of data, such as messages, from alteration.
- **Authentication protocols:** Use of cryptographic algorithms designed to authenticate the identity of entities.

Symmetric encryption and decryption


Attacker
Alice
Bob
Alice knows key K and message M
Bob knows key K
Alice encrypts M with K creating E(M,K)
Alice sends E(M,K) to Bob
Bob receives E(M,K)
Eve sees only E(M,K) and cannot compute M because she does not know the secret key K
Bob decrypts E(M,K) with K, computing D(E(M,K),K), and obtains M

The (private) key is hiding factor

Asymmetric encryption and decryption


Attacker
Alice
Bob
Alice knows Bob's public key K_{PUB_B}
Bob's key pair consists of public key K_{PUB_B} and private key K_{PRIV_B}
Alice encrypts M with using Bob's public key creating $E(M,K_{PUB\_B})$
Alice sends $E(M,K_{PUB\_B})$ to Bob
Bob receives E(M,K)
Eve sees only $E(M,K_{PUB\_B})$ and cannot compute M because she does not know Bob's private key K_{PRIV_B}
Bob uses his private key K_{PRIV_B} to decrypt the encrypted message, computing $D(E(M,K_{PUB\_B}), K_{PRIV\_B}$ and obtaining message M

The public and private keys are hiding factors

Advantages and disadvantages

Advantages of symmetric encryption: (i) A system that possesses the secret key can only decrypt a message, (ii) It is faster.

Disadvantages of symmetric encryption: (i) The secret key is to be transmitted to the receiving system before the actual message is to be transmitted, (ii) It cannot provide digital signatures that cannot be repudiated.

Advantages of asymmetric encryption: (i) There is no need for exchanging keys, thus eliminating the key distribution problem, (ii) It can provide digital signatures that can be repudiated.

Disadvantages of asymmetric encryption: (i) It is slower.

Symmetric versus asymmetric key cryptography

Symmetric key cryptography uses symmetric encryption and decryption algorithms. On the other hand, the asymmetric key cryptography comprises asymmetric encryption and decryption algorithms.

Symmetric key cryptography	**Asymmetric key cryptography**
1. It follows the principle of sharing secrecy.	1. It follows the principle of personal secrecy.
2. It permutes or substitutes the plaintext.	2. It manipulates the plaintext.
3. It uses only the private key.	3. It uses both public and private keys.
4. This is also known as private-key cryptography.	4. This is also known as public-key cryptography.

Note: If the public and private keys are same in an asymmetric encryption it will not reduce to a symmetric encryption.

Categories of attacks

Information can be attacked in broadly two ways – passive attack and active attack. However, there are some general attacks that cannot be classified like this.

Definition (Passive attack)

The attack where others' contents are read but not modified.

Definition (Active attack)

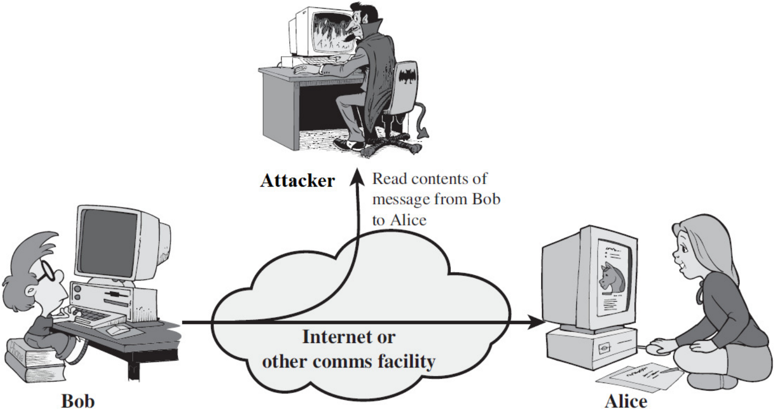
The attack where others' contents are read and modified.

Categories of attacks

The various types of attacks are listed below.

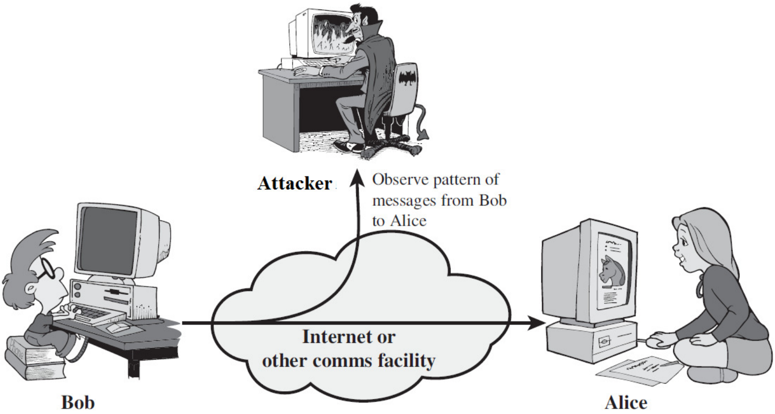
- Passive attacks
  1. Release of message contents
  2. Traffic analysis
  3. Side-channel attack
- Active attacks
  1. Masquerade
  2. Replay
  3. Modification of messages
  4. Denial of service

Passive attacks


Attacker
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

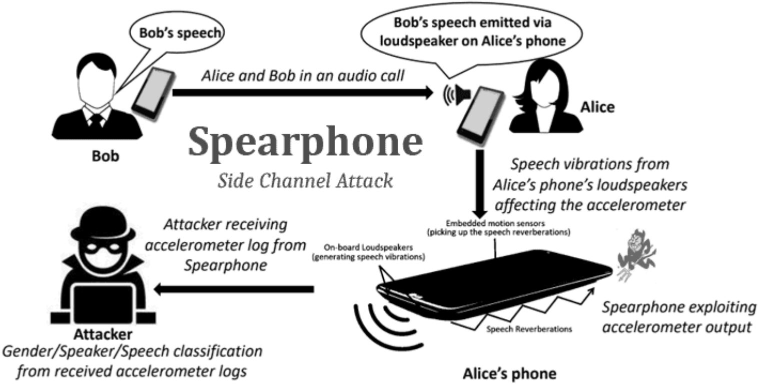
Release of message contents

Passive attacks


Attacker
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

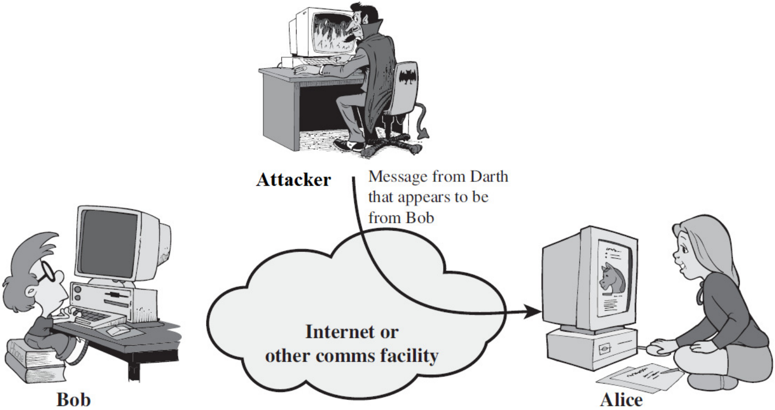
Traffic analysis

Passive attacks


Bob's speech
Bob's speech emitted via loudspeaker on Alice's phone
Alice and Bob in an audio call
Bob
Alice
Spearphone
Side Channel Attack
Speech vibrations from Alice's phone's loudspeakers affecting the accelerometer
Attacker receiving accelerometer log from Spearphone
Embedded motion sensors (picking up the speech reverberations)
On-board Loudspeakers (generating speech vibrations)
Speech Reverberations
Spearphone exploiting accelerometer output
Attacker
Gender/Speaker/Speech classification from received accelerometer logs
Alice's phone

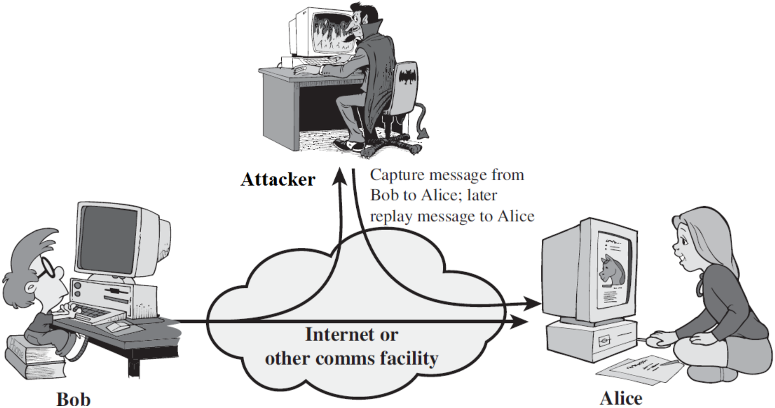
Side-channel attack

Active attacks


Attacker
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

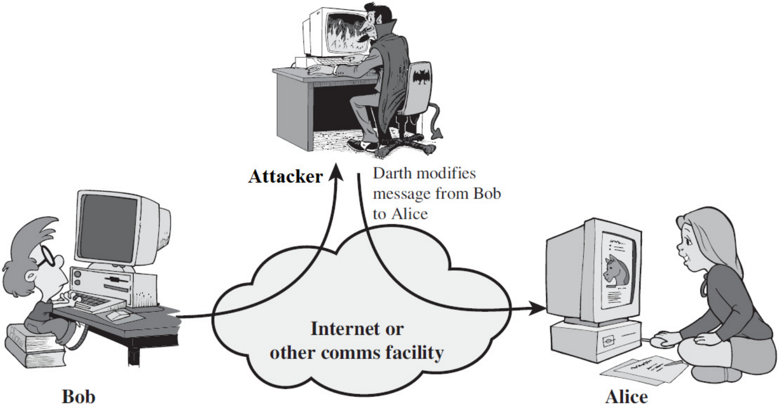
Masquerade

Active attacks


Attacker
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

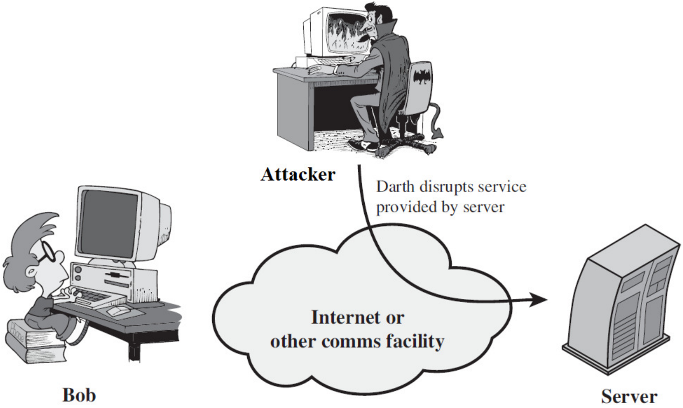
Replay

Active attacks


Attacker
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Modification of messages

Active attacks


Attacker
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

Denial of service

Basics of vulnerabilities

A vulnerability is a system susceptibility or flaw leading to the insecurity of information. Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities.

An *exploitable vulnerability* is one for which at least one working attacks exists.

Backdoors

A backdoor in a cryptosystem or an algorithm is any secret method of bypassing normal authentication or security controls, while attempting to remain undetected.

Note: Backdoor is also referred to as trapdoor in the literature.

Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between the sender and the receiver.

Eavesdropping can be done over telephone lines (wiretapping), email, instant messaging, and other methods of communication considered as private.

Spoofing

Spoofing of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data.

Spoofing can be of different types as follows:

- Referrer spoofing
- Caller ID spoofing
- E-mail address spoofing
- GPS spoofing

Tampering

Tampering describes an intentional modification of information in a way that would make them harmful to the owner (both sender and receiver).

This threat has prompted manufacturers to make products that are either difficult to modify or at least difficult to modify without warning the consumer that the product has been tampered with.

Repudiation

Repudiation describes a situation where the authenticity of a signature is being challenged.

A repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions.

Information disclosure

Information disclosure (privacy breach or data leak) describes a situation where information, thought to be secure, is released in an untrusted environment.

Information disclosure enables an attacker to gain valuable information about a system. Therefore, it is always important to consider what information you are revealing and whether it can be used by a malicious user.

Resources

Books:

1. Bruce Schneier, Applied Cryptography, John Wiley & Sons, Second Edition, 1996.
2. Wenbo Mao, Modern Cryptography Theory and Practice, Prentice Hall, 2004.
3. Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, CRC Press, 2007.

Journals:

1. IEEE Transactions on Information Theory, IEEE.
2. ACM Transactions on Information and System Security, ACM.
3. Journal of Cryptology, Springer.
4. Designs, Codes and Cryptography, Springer.

Resources

Popular courses:

1. Dan Boneh at Stanford – http://crypto.stanford.edu/∼dabo/index.html#courses, https://www.coursera.org/course/crypto
2. Ron Rivest at MIT – http://courses.csail.mit.edu/6.897/spring04, http://courses.csail.mit.edu/6.857/2013
3. Salil Vadhan at Harvard – http://people.seas.harvard.edu/ salil/cs127
4. Rafael Pass at Cornell – http://www.cs.cornell.edu/courses/cs487/2007fa