**Lecture 1 Notes**

Slide 4

* Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.
* The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing."
* In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.
* These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

Slide 6

* Cryptography is closely related to the disciplines of [cryptology](https://searchsecurity.techtarget.com/definition/cryptology) and [cryptanalysis](https://searchsecurity.techtarget.com/definition/cryptanalysis). It includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit.
* However, in today's computer-centric world, cryptography is most often associated with scrambling [plaintext](https://searchsecurity.techtarget.com/definition/plaintext) (ordinary text, sometimes referred to as cleartext) into [ciphertext](https://whatis.techtarget.com/definition/ciphertext) (a process called [encryption](https://searchsecurity.techtarget.com/definition/encryption)), then back again (known as decryption).
* Individuals who practice this field are known as cryptographers.

Slide 9

* Modern cryptography concerns itself with the following four objectives:
* **Confidentiality**: the information cannot be understood by anyone for whom it was unintended
* **Integrity:**the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
* **Non-repudiation**: the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information
* **Authentication**: the sender and receiver can confirm each other's identity and the origin/destination of the information

Slide 7

* Cryptosystems use a set of procedures known as cryptographic algorithms, or ciphers, to encrypt and decrypt messages to secure communications among computer systems, devices such as smartphones, and applications.
* A cipher suite uses one algorithm for encryption, another algorithm for message authentication, and another for key exchange.
* This process, embedded in protocols and written in software that runs on operating systems and networked computer systems, involves public and private key generation for data encryption/decryption, digital signing and verification for [message authentication](https://searchsecurity.techtarget.com/definition/message-authentication-code-MAC), and key exchange.
* Cryptosystems use a set of procedures known as cryptographic algorithms, or ciphers, to encrypt and decrypt messages to secure communications among computer systems, devices such as smartphones, and applications.
* A cipher suite uses one algorithm for encryption, another algorithm for message authentication, and another for key exchange.
* This process, embedded in protocols and written in software that runs on operating systems and networked computer systems, involves public and private key generation for data encryption/decryption, digital signing and verification for [message authentication](https://searchsecurity.techtarget.com/definition/message-authentication-code-MAC), and key exchange.

Slide 8

* **History of cryptography**
* The word "cryptography" is derived from the Greek *kryptos*, meaning hidden. The origin of cryptography is usually dated from about 2000 B.C., with the Egyptian practice of hieroglyphics.
* These consisted of complex pictograms, the full meaning of which was only known to an elite few.
* The first known use of a modern [cipher](https://searchsecurity.techtarget.com/definition/cipher) was by Julius Caesar (100 B.C. to 44 B.C.), who did not trust his messengers when communicating with his governors and officers.
* For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

Slide 10

* Let’s say there’s a person named Ram. Now suppose *Ram* sends a message to his friend *Sam* who is on the other side of the world.
* Now obviously he wants this message to be private and nobody else should have access to the message.
* He uses a public forum, for example, WhatsApp for sending this message.
* The main goal is to secure this communication.
* Let’s say there is a smart guy called *Eaves* who secretly got access to your communication channel. Since this guy has access to your communication, he can do much more than just eavesdropping, for example, he can try to change the message.
* Now, this is just a small example. What if *Eave* gets access to your private information? The result could be catastrophic.
* So how can *Ram* be sure that nobody in the middle could access the message sent to *Sam*? That’s where ***Encryption or Cryptography*** comes in.
* *let’s see how cryptography can help secure the connection between Ram and Sam.*
* So, to protect his message, *Ram* first convert his readable message to unreadable form. Here, he converts the message to some random numbers. After that, he uses a key to encrypt his message, in Cryptography, we call this [***ciphertext***](https://en.wikipedia.org/wiki/Ciphertext).
* *Ram* sends this *ciphertext* or encrypted message over the communication channel, he won’t have to worry about somebody in the middle of discovering his private messages. Suppose, *Eaves* here discover the message and he somehow manages to alter it before it reaches *Sam*.
* Now, Sam would need a key to decrypt the message to recover the original plaintext. In order to convert the ciphertext into plain text, Sam would need to use the decryption key. Using the key he would convert the ciphertext or the numerical value to the corresponding plain text.
* After using the key for decryption what will come out is the original plaintext message, is an error. Now, this error is very important. It is the way Sam knows that message sent by Ram is not the same as the message that he received. Thus, we can say that encryption is important to communicate or share information over the network.