An Introduction to Cryptography

Course Glossary

Throughout the course, you might find some new words, phrases and abbreviations being used – you can always come to this document to look up any unfamiliar terms!

Word	Definition
Asymmetric	In the context of cryptography, asymmetric refers to the keys used to encrypt and decrypt a message being different.
Cipher	A cipher is a secret code, usually one that's created using a mathematical algorithm.
Ciphertext	Ciphertext is encrypted text transformed from plaintext using an encryption algorithm.
Cryptography	Cryptography, or cryptology is the practice and study of techniques for secure communication in the presence of adversarial behaviour.
Integrity	The state of being whole (intact) and undivided.

Keyspace	Keyspace for an algorithm refers to the set of all possible keys that can be used.
Permutation	The action of changing the arrangement, especially the linear order, of a set of items.
Plaintext	Plaintext is usually ordinary readable text before it is encrypted into ciphertext, or readable text after it is decrypted.
Privacy	The state of being free from public attention.
Security	The state of being free from danger or threat.
Substitution	The action of replacing something with thing else.
Symmetric	In the context of cryptography, symmetric refer to the keys used to encrypt and decrypt a message being the same.
Transposition	Transposition is the action of changing the order of some ordered sequence.