- Cryptography is the technique message from a non-readable format back to a readable format without knowing how they initially converted from readable format to non-readable format.
- Cryptography is heavily based on mathematical theory and computer science practice, cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.
- 3. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means.
- These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted.
- 5. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.
- Cryptography or cryptology (from Greek κρυπτός kryptós, "hidden, secret"; and γράφειν graphein, "writing", or -λογία -logia, "study", respectively) is the practice and study of techniques for secure communication in the presence of third parties called adversaries.
- More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.
- 8. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering.
- 9. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

- 10. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.
- 11. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means.
- 12. The growth of cryptographic technology has raised a number of legal issues in the information age.
- 13. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.
- 14. In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation
- 15. Cryptography also plays a major role in digital rights management and copyright infringement of digital media.

Related Posts:

- 1. Types of Attack
- 2. Security threats
- 3. Computer and cyber security
- 4. Introduction to network security
- 5. Intrusion detection tool
- 6. Categories of security assessments
- 7. Security terminologies and principals
- 8. Intoduction to intrusion
- 9. Intrusion detection tool
- 10. Categories of security assessments
- 11. Intrusion terminology
- 12. Cryptography attacks

- 13. SSH
- 14. MD5
- 15. Message digest functions
- 16. Digital signature
- 17. Authentication Functions
- 18. One way hash function
- 19. Hash function in network web security
- 20. Digital signature standard
- 21. SSL Secure socket layer