1. Kryptographie ist die Wissenschaft der Verschlüsselung und Entschlüsselung von Informationen.
2. Verschlüsselung bedeutet, Daten in eine unverständliche Form zu überführen, um sie vor unbefugtem Zugriff zu schützen.
3. Beispiel: Verschlüsselung von Passwörtern in einer Datenbank, um sie vor Diebstahl zu schützen.
4. Kryptografie ist wichtig, um die Vertraulichkeit, Integrität und Authentizität von Daten zu gewährleisten.
5. Ziele der Kryptografie: Vertraulichkeit, Integrität, Authentizität, Nicht-Abstreitbarkeit.
6. Beispiele für Kryptografie-Verfahren: RSA, AES, DES.
7. Kryptographie bezieht sich auf Verschlüsselung und Entschlüsselung, während Kryptologie ein breiterer Begriff ist, der auch verwandte Disziplinen einschließt.
8. Kryptografie kommt in der IT-Sicherheit, Online-Kommunikation, Finanztransaktionen und vielen anderen Bereichen zum Einsatz.
9. Das Ziel von Kryptografie ist der Schutz von Informationen vor unbefugtem Zugriff.
10. Die Sicherheit von Kryptografie hängt von der Stärke der verwendeten Algorithmen und Schlüssellängen ab.
11. Der Name "Kryptographie" stammt aus dem Griechischen und bedeutet "geheimes Schreiben".
12. Kryptografie wird durch Verwendung eines Schlüssels entschlüsselt, der den Zugang zu den verschlüsselten Daten ermöglicht.
13. Die Kryptografie hat eine lange Geschichte und wurde in verschiedenen Kulturen zur Geheimhaltung von Informationen eingesetzt.
14. In der Kryptografie ist ein Schlüssel eine spezielle Information, die zur Verschlüsselung und Entschlüsselung verwendet wird.
15. Es gibt kein "sicherstes" Verschlüsselungsverfahren, aber aktuell als stark gilt AES mit ausreichend langer Schlüssellänge.
16. Aktuell genutzte Verschlüsselungsverfahren umfassen RSA, AES, ECC.
17. 256 Bit Sicherheit gilt als sehr sicher und bietet einen starken Schutz vor Brute-Force-Angriffen.
18. Kryptografie muss angewendet werden, wenn Vertraulichkeit, Integrität oder Authentizität von Daten gewährleistet werden müssen.
19. Kryptografie schützt Daten durch Verschlüsselung, während Steganographie Informationen versteckt, um ihre Existenz zu verschleiern.
20. Private Schlüssel dienen der Entschlüsselung, öffentliche Schlüssel der Verschlüsselung von Daten.
21. Es gibt viele Verschlüsselungsverfahren, aber häufig genutzte Standards sind AES-256, RSA-2048.
22. Daten werden verschlüsselt, indem ein Algorithmus und ein Schlüssel verwendet werden.
23. Der Cäsar Code kann durch systematisches Durchprobieren aller möglichen Verschiebungen entschlüsselt werden.
24. Die Dauer, ein 256 Bit Passwort zu knacken, hängt von der Rechenleistung und den verwendeten Techniken ab.
25. Ein 128 Bit Schlüssel wird in der Kryptografie für Verschlüsselungsalgorithmen wie AES verwendet.
26. Die Zeit, eine 128 Bit-Verschlüsselung zu knacken, hängt von der Rechenleistung ab; AES ist ein weit verbreiteter Verschlüsselungsalgorithmus.
27. 256 Bit entsprechen 32 Zeichen in einer Hexadezimaldarstellung.
28. Das Verschlüsseln von E-Mails ist ratsam, um die Privatsphäre und Sicherheit der Kommunikation zu schützen.
29. Die stärkste Verschlüsselung hängt von der Verwendung ab; AES mit ausreichender Schlüssellänge wird oft als sehr sicher betrachtet.
30. AES (Advanced Encryption Standard) verschlüsselt Daten mithilfe eines Schlüssels und eines Substitutions-Permutations-Netzwerks.
31. Die Ziele der Kryptografie sind Vertraulichkeit, Integrität, Authentizität und Nicht-Abstreitbarkeit.
32. Handys können durch Einstellungen im Betriebssystem verschlüsselt werden, um Daten zu schützen.
33. Steganographie ist die Kunst, Informationen zu verbergen, während Kryptographie die Kunst ist, Informationen zu verschlüsseln und zu schützen.