12. Mögliche Antworten zu den Kryptographie- und Steganographie-Fragen

1. Was ist Kryptographie?

Kryptographie ist eine Wissenschaft zur Entwicklung von Kryptosystemen und neben der Kryptoanalyse ein Teilgebiet der Kryptologie. Mit Hilfe kryptographischer Verfahren wie Verschlüsselung sollen Daten vor unbefugtem Zugriff geschützt und sicher ausgetauscht werden.

2. Was bedeutet Verschlüsselung?

Verschlüsselung ist heute hauptsächlich ein Begriff aus der IT. Daten, E-Mails, Computer etc. werden verschlüsselt. Doch das war nicht immer so. Die Verschlüsselung hat ihren Ursprung bereits im Jahre 480. Doch hier gab es natürlich noch keine IT, die es zu verschlüsseln galt. Die Verschlüsselung war bis vor einigen Jahren noch ein Tool, welches hauptsächlich in der

3. Beschreiben Sie mit einem gewählten Beispiel die Kryptographie?

Alice möchte Bob eine Nachricht über das Internet schicken. Da dies ein unsicherer Kanal ist, könnte die Botschaft jeder mitlesen. Die neugierige Eve lauert schon darauf, die Botschaft abzufangen. Alice ist daher schlau und überträgt ihre Nachricht verschlüsselt an Bob. Wie macht sie das?

- **Alice benutzt ein Verschlüsselungsverfahren, das ihre Nachricht in einen Geheimtext verwandelt. Das Verfahren besteht aus einer Sammlung mathematischer Schritte, auch Algorithmus genannt.**
- **Bei dem Verfahren wendet sie zusätzlich einen geheimen Schlüssel an.**
- **Die neugierige Eve ärgert sich: Da der Text in einen Geheimtext verwandelt wurde, kann sie nur eine unverständliche, scheinbar chaotische Zeichenfolge sehen.**
- **Damit Bob die Botschaft lesen kann, entziffert er den Geheimtext wiederum mit einem Entschlüsselungsverfahren.**
- **Dabei wendet er den gleichen Schlüssel an, den Alice bereits verwendet hat.**

Da Alice und Bob den gleichen geheimen Schlüssel verwenden, spricht man von symmetrischer Verschlüsselung oder auch „Secret-Key-Verfahren". Damit das Ganze funktioniert, müssen Alice und Bob vorher den Schlüssel untereinander austauschen, was jedoch eine riskante Angelegenheit ist.

4. Warum ist Kryptografie wichtig?

Kryptowährungen beruhen rein auf kryptografischen Konzepten. Bitcoin wurde von einer Person (oder einer Gruppe) mit dem Pseudonym Satoshi Nakamoto erfunden, der seinen Ansatz in Form eines Whitepapers formulierte, das er 2009 in einem Kryptografie-Forum veröffentlichte.

Das schwierigste Problem, das Nakamoto löste, war das sogenannte „Double-Spend"-Problem. Bitcoin existiert nur in Form von Codezeilen. Wie kann also verhindert werden, dass Bitcoin-Besitzer ihr Geld einfach kopieren und ausgeben? Die Lösung, die Nakamoto ersann, beruhte auf einer wohlbekannten Verschlüsselungsmethode, die Public-Key-Verschlüsselungsverfahren genannt wird.

Bitcoin (genau wie Ethereum und viele andere Kryptowährungen) nutzt eine Technologie namens Public-Key-Verschlüsselungsverfahren, das auf öffentliche (Public) und private (Private) Schlüssel setzt. Dadurch sind diese Kryptowährungen.

5. Was sind die 4 Ziele der Kryptographie?

Die heutige Kryptographie beinhaltet vier große Ziele zum Schutz von Informationen: Vertraulichkeit/ Zugriffsschutz, Integrität/ Änderungsschutz, Authentizität/ Fälschungsschutz, Verbindlichkeit/ Nichtabstreitbarkeit.

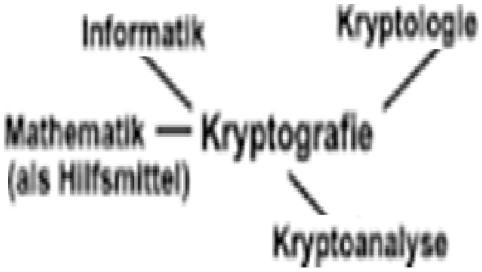
6. Welche Kryptographie Verfahren gibt es?

In der modernen Kryptographie werden hauptsächlich drei Verschlüsselungsverfahren unterschieden:

- **Symmetrische Kryptographie. Bei der symmetrischen Kryptographie wird ein einziger Schlüssel zum Ver- und Entschlüsseln einer Nachricht benutzt. ...**
- **Asymmetrische Kryptographie. ...**
- **Hybride Kryptographie.**

7. Was ist der Unterschied zwischen Kryptographie und Kryptologie?

Kryptologie ist die Kunst und Wissenschaft, Methoden zur Verheimlichung von Nachrichten zu entwickeln. Die Kryptografie oder Kryptographie ist ein Teil der Kryptologie und die Wissenschaft zur Entwicklung von Kryptosystemen, die die Geheimhaltung von Nachrichten zum Ziel haben.



8. Wo kommt Kryptographie zum Einsatz?
Kryptographie wird in vielen Anwendungen wie Banktransaktionen, Computer-kennwörter und E-Commerce-Transaktionen verwendet. Drei Arten von kryptografischen Techniken im Allgemeinen verwendet.

9. Was ist das Ziel von Kryptographie?
Es handelt sich bei der Kryptographie um die Wissenschaft, Methoden, Werkzeuge und Algorithmen zu entwickeln, mit deren Hilfe sich Daten chiffrieren und für Unbefugte unkenntlich machen lassen. Diese sollen den unberechtigtem Zugriff auf Informationen verhindern und einen sicheren Datenaustausch ermöglichen.

10. Wie sicher ist Kryptographie?
Erst wenn es nach ca. fünf Jahren nachweisbar viele Kryptografie-Spezialisten nicht geschafft haben, das neue kryptografische Verfahren zu brechen, gilt ein kryptografisches Verfahren als praktisch sicher. Allerdings werden immer wieder solche Verfahren auch nach den fünf Jahren von Mathematikern gebrochen.

11. Wie entstand und woher kommt der Name 'Kryptographie' genau?
Die Silbe „Krypto“ im Wort „Kryptowährung“ stammt aus dem Griechischen und bedeutet „geheim“ und 'graph' bedeutet Sprache, womit eben Kryptographie geheime Sprache bedeutet!

12. Wie entschlüsselt man Kryptographie?
Um einen Geheimtext wieder zu entschlüsseln oder eine Nachricht zu signieren, wird der private Schlüssel benötigt. Im Gegensatz zu symmetrischen Verfahren, bei denen sich mehrere Benutzer einen geheimen Schlüssel teilen, verfügt bei asymmetrischen Verfahren nur ein Benutzer über den privaten (geheimen) Schlüssel.

13. Wie entstand die Kryptographie?
1900 vor Chr. verwendeten ägyptische Schriftgelehrte bei den Inschriften eines königlichen Grabes spezielle Hieroglyphen, dies ist die erste schriftlich dokumentierte Kryptographie. Ob vor den alten Ägyptern schon andere Völker Kryptographie angewandt haben, ist bisweilen noch nicht bekannt.

14. Was ist ein Schlüssel in der Kryptographie?
Ein kryptografischer Schlüssel ist eine Zeichenfolge, die in einem Verschlüsselungs-algorithmus verwendet wird, um Daten so zu ändern, dass sie zufällig erscheinen.

15. Was ist das sicherste Verschlüsselungsverfahren?
Wenn es um Datenverschlüsselung geht, bleibt die AES-Verschlüsselung (Advanced Encryption Standard) unbestreitbar eines der sichersten und am weitesten verbreiteten Systeme der Welt.

16. Welche Verschlüsselungsverfahren werden aktuell genutzt?
Wichtige Meilensteine in der Entwicklung neuer Verschlüsselungsverfahren stellen die Erfindung des Telegraphen, des Computers und der asymmetrischen Kryptosysteme dar. Das heute aufgrund der digitalen Kommunikation am weitesten verbreitete Verfahren ist das RSA-Verfahren.

17. Wie sicher ist 256 Bit Sicherheit?
Da es sich bei AES-256 um ein symmetrisches Verschlüsselungsverfahren handelt, sind die einzelnen Schlüssel zum Ver- und Entschlüsseln identisch. Der Wert 256 steht dabei für die Schlüssellänge, in diesem Fall 256 Bit. Mit dieser Länge gilt AES-256 als ein besonders sicherer Standard.

18. In welchem Fall muss Kryptographie angewendet werden?
Er ist nötig, um einen Klartext zu ver- oder zu entschlüsseln. Meistens gibt das Verfahren vor, wie der Schlüssel aussehen kann. Bei dieser Art der Verschlüsselung werden einzelne Zeichen des Klartextes durch andere Zeichen eines Schlüsselalphabets ersetzt.

19. Was ist der Unterschied zwischen Steganographie und Kryptographie?
20. Was sind private und öffentliche Schlüssel?
21. Wie viele Verschlüsselungen gibt es?
22. Wie geht verschlüsseln?
23. Wie kann man den Cäsar Code knacken?
24. Wie Länge dauert es ein 256 Bit Passwort zu Knacken?
25. Was ist ein 128 Bit Schlüssel?
26. Wie Länge dauert es eine 128 Bit Verschlüsselung zu knacken und was genau ist AES-Verschlüsselung?
27. Wie viele Zeichen sind 256 Bit?
28. Sollte man E-Mails verschlüsseln?
29. Was ist die stärkste Verschlüsselung?
30. Wie verschlüsselt AES?

31. Was sind die 4 Ziele der Kryptographie?

32. Wie kann ich mein Handy verschlüsseln?

33. Was versteht man unter Steganographie?