Inhaltsverzeichnis

Ethisches Hacken

Grundidee und Zweck

- Ethical Hacking nutzt dieselben Methoden wie Bedrohungsakteure, jedoch mit Erlaubnis und zum Schutz des Systems.
- **Ziel**: Schwachstellen identifizieren, bevor sie von Angreifern ausgenutzt werden.
- Teil professioneller Netzwerksicherheits- und Penetrationstests.

Eingesetzte Methoden und Vorgehen

- Nutzung von Penetrationstest-Tools, die auch von Angreifern missbraucht werden könnten.
- Angreifertechniken werden kontrolliert simuliert, um Sicherheitsmaßnahmen zu überprüfen.
- Fokus auf das Erkennen typischer Angriffskategorien wie:
    - Aufklärungsangriffe (Recon)
    - Zugriffsangriffe
    - Social Engineering
    - DoS/DDoS
    - Malware-basierte Angriffe
- Recon: Informationsbeschaffung über ein Ziel
    - Welche Systeme existieren?
    - Welche Dienste laufen dort?
    - Welche Schwachstellen können ausgenutzt werden?

Typische Werkzeuge

- Spezialisierte Tools für:
    - Netzwerk-Scanning
    - Schwachstellenanalyse
    - Exploitation
    - Passwort-Cracking
    - Analyse von Malware
- Viele Tools sind dual-use (können ethisch oder illegal eingesetzt werden).

Typische Sicherheitsmaßnahmen, die geprüft werden

- Passwortsicherheit und Richtlinien
- Physischer Zugriffsschutz
- Patch-Management
- Schutz durch Firewalls, VPNs, IPS, Antivirenlösungen
- Abschalten unnötiger Dienste/Ports
- Verschlüsselung und sichere Authentifizierung (z. B. MFA, HMAC)

Kryptographie

- Sichere Kommunikation über unsicheren Kanal
- **Hashing**: Leicht ausführbar -> schwer umkehrbar

CIA-Triade

- **Vertraulichkeit** (**C**onfidentiality)
  - Gewährleistung der Privatsphäre; nur Empfänger kann lesen
  - Realisiert z.B. durch Verschlüsselung
- **Integrität** (**I**ntegrity)
  - Sicherstellung, dass die Nachricht auf dem Weg nicht geändert wurde
  - Realisiert z.B. durch Prüfsummen
- **Authentifizierung** (**A**uthenticity)
  - Sicherstellen, dass es tatsächlich der angepriesene Absender war
  - Realisiert z.B. durch eine PIN

Beispielmethoden, um Code zu knacken

- **Brute-Force**: Alle möglichen Schlüssel probieren
- **Known-Plaintext-Methode**: Teilstück, das enthalten ist, ist bekannt (Enigma)

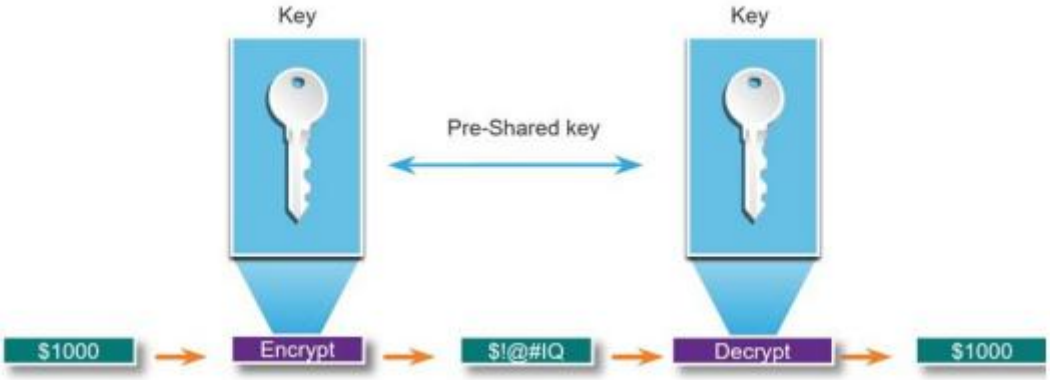
Chiffren

- **Chiffre**: Verschlüsselungsverfahren, das Klartext in Chiffretext umwandelt
- Kann nur mit dem passenden Schlüssel gelesen werden

Arten

Kategorie	**Beschreibung**	**Beispiele**
Transpositions-Chiffren	Umordnung der Zeichen	Umkehrung, Gitterzaun
Substitutions-Chiffren	Ersetzen von Zeichen	einfache Substitution
Blockchiffren	Verschlüsselung blockweise	DES, AES
Stromchiffren	Verschlüsselung bit-/byteweise	Stromchiffren allgemein
Symmetrische Chiffren	gleicher Schlüssel	DES, 3DES, AES
Asymmetrische Chiffren	Schlüsselpaar (öffentlich/privat)	RSA, PKI

Symmetrische Verschlüsselung



- Selber Schlüssel beim ver- und entschlüsseln
- Ein Schlüssel pro Kommunikationsweg zwischen zwei Personen
    - Bei vielen Kommunikationspartnern wird die Anzahl der benötigten Schlüssel sehr hoch
- **Beispiel**: Caesar / Monoalphabetische Substitution
    - Buchstaben/Bytes werden durch einen anderen ersetzt
    - Leicht zu knacken durch Muster und Statistik
- **Schneller** als asymmetrische Verschlüsselung
- Beispiele: AES & DES
- **Schlüsselaustauschproblem**: beide Parteien benötigen den gleichen Schlüssel für ver- und entschlüsseln -> Übertragung muss auf sicherem Weg erfolgen
    - **Lösung**: Asymmetrische Verschlüsselung zum Austausch des Schlüssels

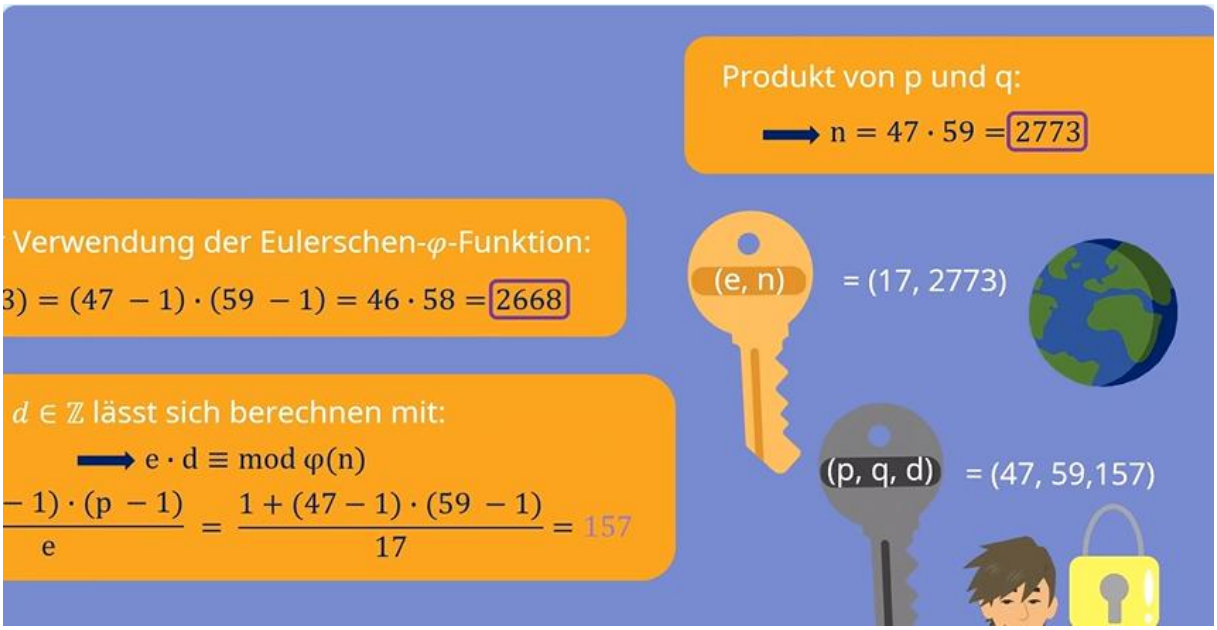
AES: Advanced Encryption Standard

- Aus dem Schlüssel werden Rundschlüssel erstellt
- Datenblock wird in Matrix geschrieben
- Mehrere Runden folgende vier Schritte über jede Datenblockmatrix
    1. Substitution: Jedes Byte wird mittels S-Box durch anderen Wert ersetzt
    2. Shift-Row: Zeilen werden um bestimmte Anzahl verschoben
    3. Mix Column: Spalten werden durch Matrixmultiplikation vermischt
    4. Key Addition: Block wird mit Rundschlüssel über XOR verknüpft

Asymmetrische Verschlüsselung

- Öffentlicher Schlüssel zum verschlüsseln
- Privater Schlüssel zum entschlüsseln
- **Langsamer** als symmetrische Verschlüsselung
- Sicherer Schlüsselaustausch
- **Beispiele**: RSA & DAS
- **Authentizität beweisen**: Wenn A mit dem eigenen privaten Schlüssel verschlüsselt und B mit dem öffentlichen Schlüssel von A entschlüsselt, beweist A, dass er im Besitz des privaten Schlüssels ist.

RSA

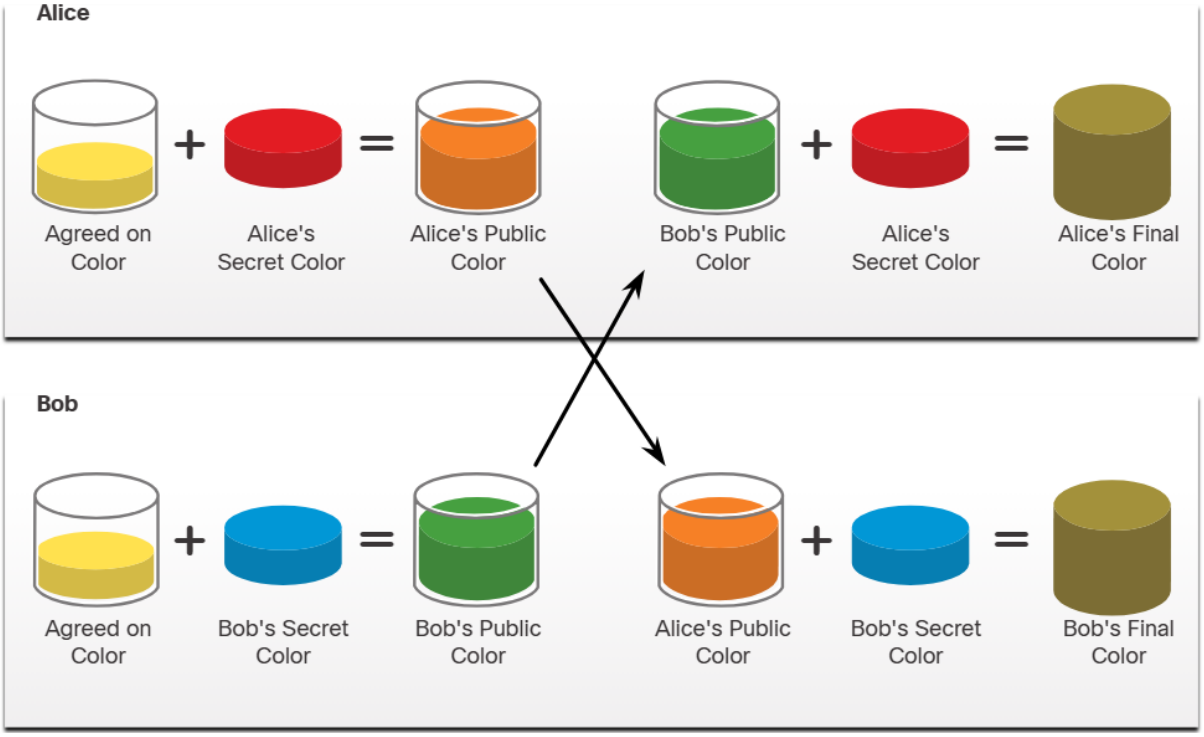


- Öffentlicher Schlüssel
  - n: Gemeinsamer Bestandteil von Public und Private (p*q=n)
  - e: Öffentlicher Exponent
- Privater Schlüssel
  - d: privater Exponent – wird aus p & q berechnet
  - p & q: Geheime Primzahlen

Hybride Verschlüsselung

- Nutzt symmetrische und asymmetrische Verschlüsselung
- **Effizienz**: Symmetrische Verschlüsselung für Datenübertragung (schnell)
- **Sicherheit**: Asymmetrische Verschlüsselung für sicheren Schlüsselaustausch
- Ablauf
    - Daten werden mit symmetrischem Schlüssel verschlüsselt
    - Symmetrischer Schlüssel wird asymmetrisch verschlüsselt
- **Beispiele**: HTTPS & verschlüsselte Mails

Diffie Hellman



Farben sollen verschiedene große Zahlenfolgen darstellen

- Es wird sich zuerst auf eine gemeinsame Zahl geeinigt
- Anschließend verrechnet jede Seite eine eigene geheime Zahl mit der öffentlichen bekannten Zahl
- Die daraus resultierenden Ergebnisse werden ausgetauscht
- Durch das Verrechnen des Ergebnisses des Partners mit der eigenen geheimen Zahl wird die Finale Zahl berechnet. Diese ist bei beiden Partnern gleich.

Shenjas Fragenkatalog

Prio	Frage	Antwort
1	Wie verbreitet sich ein Virus?	Ein Virus verbreitet sich, indem er sich in andere Programme einfügt und durch deren Ausführung weitergetragen wird.
1	Wie verbreitet sich ein Wurm?	Ein Wurm verbreitet sich selbstständig über Netzwerkschwachstellen.
1	Was ist ein Trojaner?	Ein Trojaner tarnt sich als legitime Software und führt im Hintergrund Schadcode aus.
1	Was ist Ransomware?	Ransomware blockiert den Zugriff auf Systeme oder Daten und fordert ein Lösegeld für die Freigabe.
1	Was ist ein Aufklärungsangriff (Recon)?	Ein Aufklärungsangriff dient der Informationssammlung über Systeme, Dienste oder Schwachstellen. Recon erkennen und erklären können
1	Was ist ein DoS-Angriff?	Ein DoS-Angriff unterbricht Netzwerkdienste durch übermäßigen Traffic oder manipulierte Pakete.
1	Was ist ein DDoS-Angriff?	Ein DDoS-Angriff wird von vielen koordinierten Quellen gleichzeitig durchgeführt.
1	Was bedeutet Authentifizierung?	Authentifizierung stellt sicher, dass die Identität des Absenders einer Nachricht echt ist.
1	Was ist ein Hash?	Ein Hash ist eine kurze Prüfsumme fester Länge, die aus Daten berechnet wird und deren Integrität sicherstellt.
1	Was ist ein HMAC?	Ein HMAC ist ein Hash, der zusätzlich einen geheimen Schlüssel zur Authentifizierung nutzt.
1	Wie funktioniert symmetrische Verschlüsselung?	Sender und Empfänger verwenden denselben geheimen Schlüssel für Ver- und Entschlüsselung.
1	Wie funktioniert asymmetrische Verschlüsselung?	Es werden ein öffentlicher Schlüssel zum Verschlüsseln und ein privater Schlüssel zum Entschlüsseln verwendet.
1	Nenne ein Protokoll, das asymmetrische Verschlüsselung nutzt.	TLS (ehemals SSL) verwendet asymmetrische Verschlüsselung. RSA
1	Was ist eine Transpositionschiffre?	Eine Chiffre, bei der die Buchstaben einer Nachricht neu angeordnet werden.
1	Was ist das Ziel eines Penetrationstests?	Die Sicherheitsmaßnahmen eines Netzwerks zu überprüfen, indem Angriffe simuliert werden.
2	Was ist ein Angriffsvektor?	Ein Angriffsvektor ist ein Pfad, über den sich ein Bedrohungsakteur Zugang zu einem Server, Host oder Netzwerk verschaffen kann.
2	Was ist ein Pufferüberlauf?	Ein Pufferüberlauf nutzt eine Schwachstelle im Speicher aus, wodurch Systeme funktionsunfähig werden können.