

# Gedächtnisprotokoll Sichere Systeme SoSe 2023

---

## Aufgabe: Basisangriffe

---

- Tabelle mit Sicherheitsaspekt, Szenario und Basisangriff gegeben, wobei in allen 5 Zeilen der Tabelle ein Szenario genannt war
  - Nennung des direkt durch das Szenario verletzten Sicherheitsaspekts
  - Nennung des Basisangriffs dieses Szenarios

## Aufgabe: Firewall

---

- Tabelle mit Firewallregeln gegeben, sowie verschiedene Zugriffe genannt
  - schauen, welche Regel betrifft die Anfrage, sowie Entscheidung (allow / deny)
  - ggf. schauen, welche Regel die Antwort betrifft, sowie Entscheidung (allow / deny)
  - Gesamtentscheidung treffen (allow / deny)
- (ich glaube) Was ist ein Application Level Gateway?
- (ich glaube) Warum werden Network Level Firewalls und Application Level Gateways meist zusammengenutzt?

## Aufgabe: Biometrie

---

- FAR für eine gegebene Situation berechnen

## Aufgabe: Caesar-Verschlüsselung

---

- Chiffre, sowie Schlüssel (4) gegeben
  - Aufschreiben des verschlüsselten Alphabets (A -> E, B -> F, ...)
  - Chiffre entschlüsseln (das Ergebnis war kein gültiger Satz / Ausdruck (sehr mies, wenn man immer etwas sinnvolles erwartet))
  - Schlüsselraum angeben

## Aufgabe: Sicherheitsvorfall

---

- Artikel zu Sicherheitsvorfall gegeben
  - Betroffenenrechte angeben und erklären
  - Schutz- und Gewährleistungsziele angeben und erklären
  - 8 Gebote des Datenschutzes (was war hier die Aufgabe?)

## Aufgabe: n-Schlüssel bei symmetrischer Verschlüsselung

---

- Einmal bestimmte Anzahl Teilnehmer vorgegeben und einmal n Teilnehmer
  - Anzahl benötigter Schlüssel berechnen bzw. allgemeine Formel nennen

## Aufgabe: Signatur

---

- Liste an Schlüsseln (Private Key von Alice, Public Key von Bob, etc.) und Funktionen (Hashfunktion, Verifizierfunktion, etc.) vorgegeben
  - Eintragen in entsprechende Zeilen, in welchem Schritt welcher Schlüssel und welche Funktion benötigt wurde
  - Beispiel: Bob möchte überprüfen, ob die Nachricht von Alice kommt. Welche Schlüssel und/oder Funktionen benötigt sie?