Aufgabe 1 **(14 Punkte)**

a) Gegeben sei eine kryptographische Hashfunktion $h_1:\{0,1\}^* \rightarrow \{0,2,4\}$ sowie eine Nachricht M_0 mit Hashwert $h_1(M_0) = 4$.

Wie hoch ist die Wahrscheinlichkeit, dass bei einer weiteren Nachricht M_1 ebenfalls der Hashwert $h_1(M_1) = 4$ ist? **(6 Punkte)**

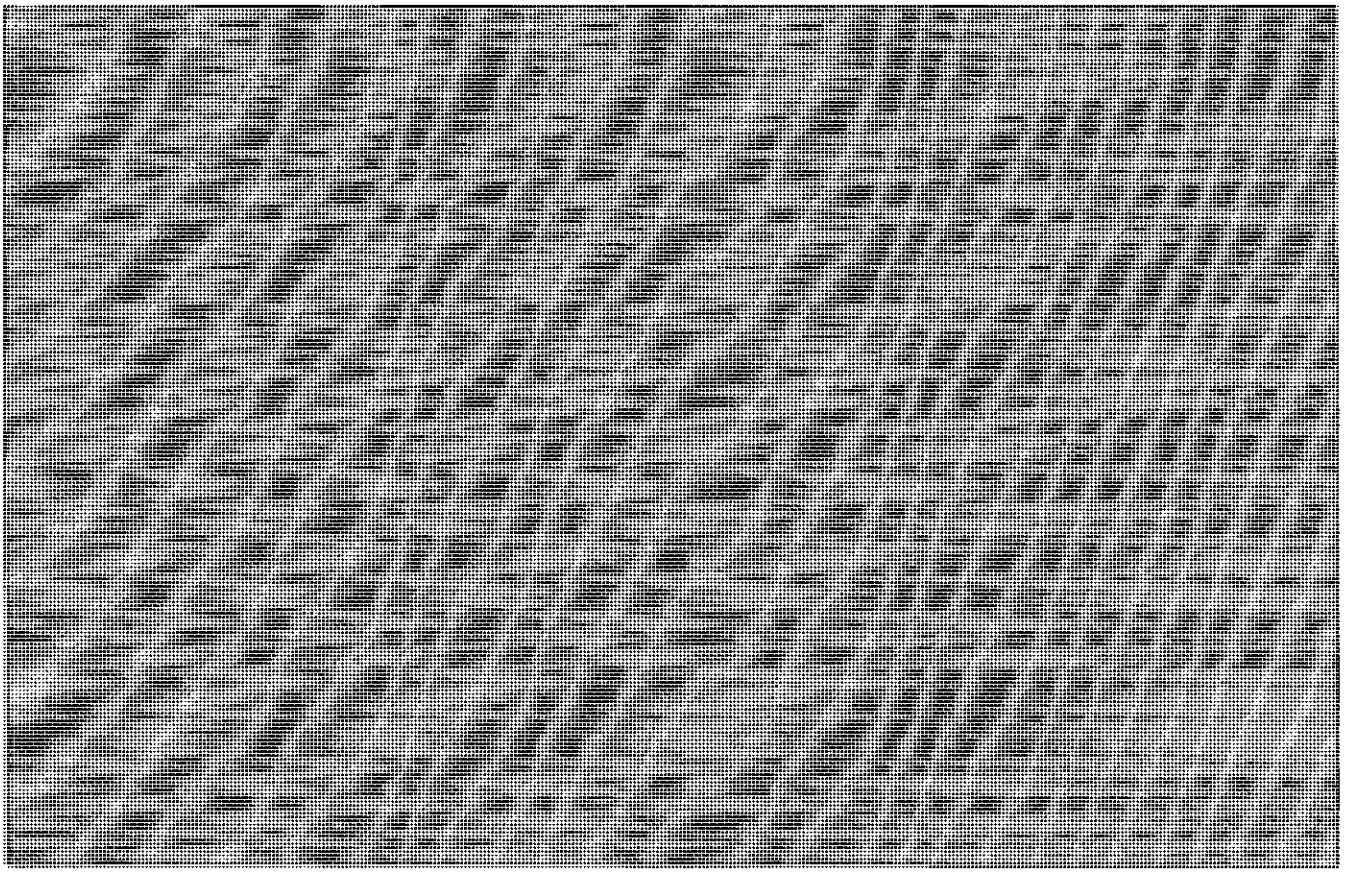
☒ 1/3

☐ 1/2

☐ 2/3

☐ 3/4

Platz für Nebenrechnungen



b) Gegeben sei eine kryptographische Hashfunktion $h_2:\{0,1\}^* \rightarrow \{0,1,2\}$ sowie eine Nachricht M_2 mit Hashwert $h_2(M_2) = 0$.

Wie hoch ist die Wahrscheinlichkeit, dass bei zwei weiteren Nachrichten M_3 und M_4 die Hashwerte $h_2(M_3)$ und $h_2(M_4)$ beide ungleich 0 sind?

(8 Punkte)

- [x] $4/9 = 2/3 * 2/3$
- [ ] $1/9 = 1/3 * 1/3$
- [ ] $1/3 = 1/2 * 2/3$
- [ ] $2/3 = 1/3 + 1/3$
- [ ] $4/3 = 2/3 + 2/3$

Platz für Nebenrechnungen

Aufgabe 2: **(9 Punkte)**

Welche der folgenden Aussagen treffen zu?

☐ Ein Virus benötigt kein Wirtsprogramm zur Verbreitung.

☒ Ein Wurm benötigt kein Wirtsprogramm zur Verbreitung.

☒ Zum Erraten eines Passworts der Länge 8 bei einem Alphabet mit 16 Zeichen braucht man im schlechtesten Fall $2^{32} = 16^8$ Versuche.

☐ Zum Erraten eines Passworts der Länge 4 bei einem Alphabet mit 32 Zeichen braucht man im schlechtesten Fall $2^{64} = 4^{32}$ Versuche.

☐ Unter SPAM versteht man unerwünschte Werbemail, die an genau einen Benutzer gesendet wird.

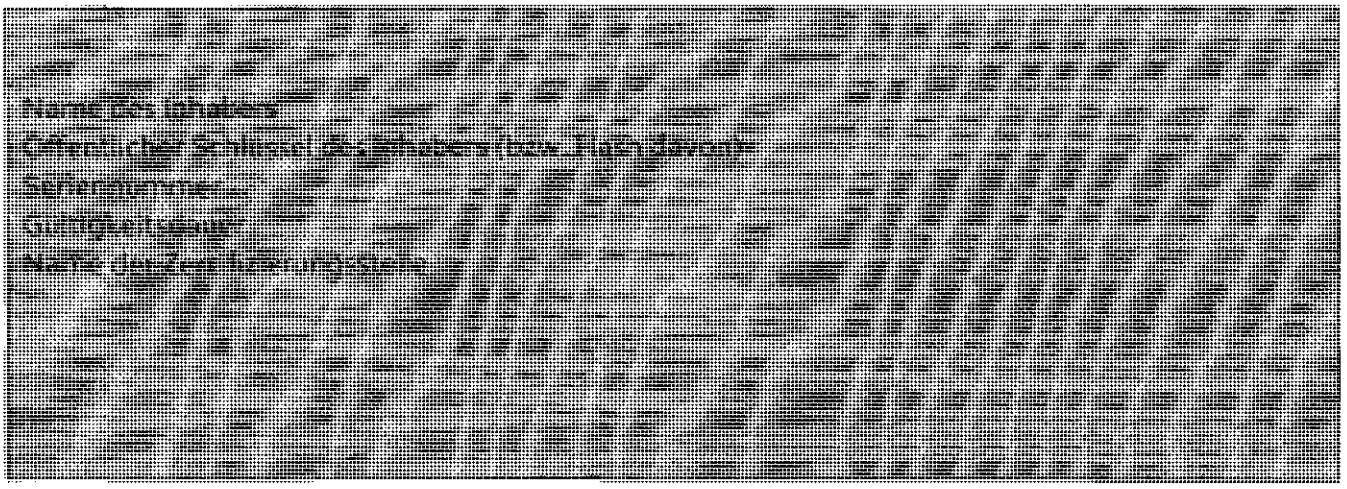
☒ Unbefugter Informationsgewinn ist in der Regel ein passiver Angriff.

☐ Unabsichtliche Bedrohungen können nur passive Bedrohungen, niemals aber aktive Bedrohungen sein.

☒ Die unbefugte Erzeugung von Nachrichten ist ein Angriff auf die Authentizität.

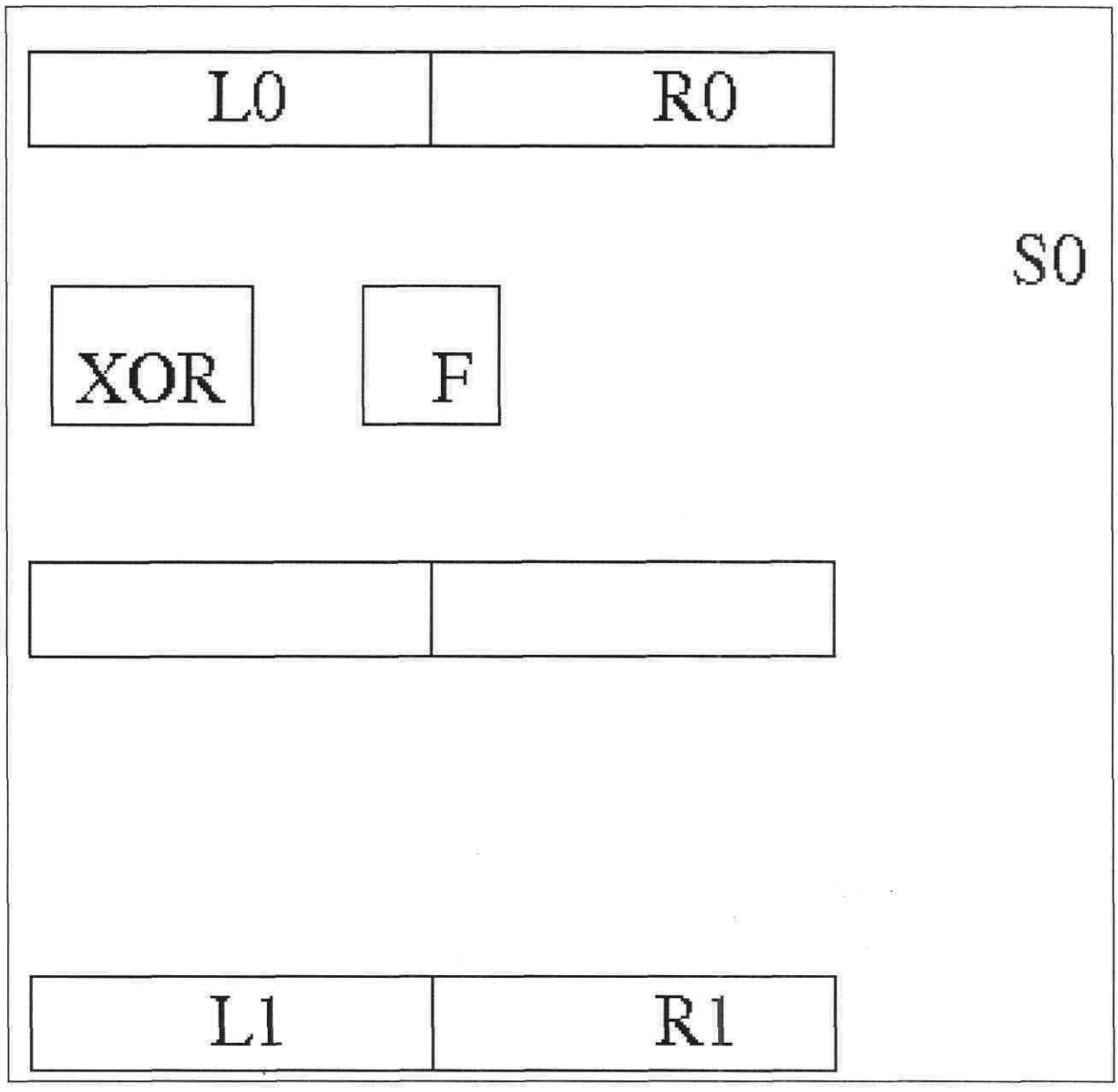
Aufgabe 3: **(14 Punkte)**

a) Nennen Sie vier Daten, die ein Zertifikat enthält. **(4 Punkte)**



b) Ergänzen Sie die folgende Zeichnung durch Pfeile zu einer Runde eines Feistel-Netzwerks.

(10 Punkte)



s. Abbildung 2.4 des Kurstextes

Aufgabe 4: **(13 Punkte)**

a) Wird ein Cookie auf einem Web-Server oder in einem Browser gespeichert?

(2 Punkte)

Cookies werden im Browser gespeichert.

b) Ein Web-Server schickt in einer Antwort auf eine Browser-Anfrage die folgende Zeile mit:

```
Set-Cookie: student=Muster; path=/stud; domain=d1.fernuni-hagen.de
```

Bei Aufruf von welchen der folgenden URLs wird der Browser seinem Request eine Zeile

```
Cookie: student=Muster
```

beifügen? (Hierbei sollen Cookies aktiviert sein.) **(9 Punkte)**

- ☐ http://www.fernuni-hagen.de/stud
- ☒ http://www.d1.fernuni-hagen.de/stud
- ☒ http://d1.fernuni-hagen.de/stud
- ☐ http://d1.fernuni-hagen.de
- ☒ http://a2.d1.fernuni-hagen.de/stud/sub
- ☐ http://d1.uni-hagen.de
- ☐ http://d1.uni-hagen.de/stud
- ☐ http://a2.d1.fernuni-hagen.de/sub

c) Wie kann verhindert werden, dass der Browser bei irgendeiner der obigen URLs ein Cookie mitsendet? **(2 Punkte)**

siehe Kurstext Abschnitt 3.3.2, Seite 128:
Man deaktiviert Cookies im Browser
Man sorgt dafür, dass der Browser (d.h. das Betriebssystem) nicht auf die cookie-Datei zugreifen kann

Aufgabe 5: **(7 Punkte)**

Welche der folgenden Aussagen treffen zu?

☐ Ein Virenscanner schützt nach der Installation dauerhaft, eine Aktualisierung der Viren-Dateien ist nicht notwendig.

☐ Nach der Übertragung einer Web-Seite mit SSL kann der Benutzer das Zertifikat des Web-Servers ansehen. Ist die Gültigkeitsdauer dieses Zertifikats abgelaufen, bedeutet dies, dass der Web-Server von Angreifern erfolgreich angegriffen und übernommen wurde.

☐ Das Programm PGP komprimiert zu versendende Nachrichten niemals vor der Verschlüsselung.

☒ Auf einem Computer, auf dem ein Web-Server ausgeführt wird, sollten keine Programme zur Software-Entwicklung, z.B. Compiler, installiert sein.

☐ Einen Computer, auf dem ein Web-Server ausgeführt wird, sollte man aus der Ferne mit Hilfe des Programms telnet administrieren.

☒ Die Erstellung einer IT-Sicherheitsleitlinie (IT security policy) erfolgt vor der Erstellung einer IT-Sicherheitskonzeption.

Aufgabe 6: **(11 Punkte)**

Gegeben sei ein Paketfilter mit der Devise "Alles was nicht explizit erlaubt ist, ist verboten" und der folgenden Regelmenge für eingehende Pakete, die in der Reihenfolge von oben nach unten abgearbeitet wird:

Absender-IP	Absender-Port	Empfänger-IP	Empfänger-Port	Aktion
*	*	10.71.144.2	23	Verbieten
*	*	10.71.144.*	23	erlauben
141.71.1.1	*	10.71.144.5	110	erlauben

Welche der folgenden Aussagen treffen zu?

☒ Ein Paket mit Empfänger-Port=24 wird auf jeden Fall verworfen.

☐ Ein Paket mit Empfänger-Port=23 wird auf jeden Fall verworfen.

☐ Ein Paket mit Absender-IP=132.176.77.130, Absender-Port=199, Empfänger-IP=10.71.144.1, Empfänger-Port=25 wird erlaubt.

☒ Ein Paket mit Absender-IP=132.176.77.130, Absender-Port=199, Empfänger-IP=10.71.144.1, Empfänger-Port=23 wird erlaubt.

☐ Ein Paket mit Absender-IP=132.176.77.130, Absender-Port=110, Empfänger-IP=10.71.144.2, Empfänger-Port=23 wird erlaubt.

☐ Ein Paket mit Absender-IP=141.71.1.1 wird auf jeden Fall erlaubt.

☐ Ein Paket mit Absender-IP=141.71.1.1 wird auf jeden Fall verworfen.

☒ Das Ändern der Devise auf „Alles was nicht explizit verboten ist, ist erlaubt" verändert das Verhalten des Paketfilters, auch wenn die Regeln selbst nicht verändert werden.

☐ Das Hinzufügen der Regel

*	24	10.71.144.1	23	verbieten

zwischen der ersten und der zweiten Regel in obiger Regelmenge ändert nichts am Verhalten des Paketfilters.

Aufgabe 7: **(14 Punkte)**

Gegeben seien bei einer RSA-Verschlüsselung die Primzahlen p=3 und q=5, der Modulus n=p*q=15 und der Exponent e=7.

a) Bestimmen Sie den Exponenten d zum Entschlüsseln durch systematisches Ausprobieren. (10 Punkte)

d= 7, da d*e=49 = 48+1 = 1 mod 8 = 1 mod (p-1)*(q-1)

b) Könnte auch der Exponent e=5 benutzt werden? (2 Punkte)

Ja ☐ Nein ☒

c) Warum nicht? (2 Punkte)

da e=5 nicht teilerfremd zu n

Platz für Nebenrechnungen

Aufgabe 8: **(18 Punkte)**

a) Nennen Sie die vier zu schützenden Eigenschaften in einem IT-System. (4 Punkte)

Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit

b) Nennen Sie zwei weitere Einteilungen von Bedrohungen neben aktiv / passiv. (4 Punkte)

Absichtlich/unabsichtlich, technisch/nicht-technisch

c) Zu welcher Klasse von Angriffen gehört das Programm crack? Erklären Sie in wenigen Sätzen, wie crack arbeitet. Welche Regeln sollte man angesichts von crack bei der Wahl seines Passwortes beachten. (10 Punkte)

Systematisches Ausprobieren bzw. Wörterbuch-Angriff auf Passwörter. S. Kurstext S. 42/43.