Securitylab - Report

Bonusmodul

Name: Minh Hieu Le

Die folgenden Aufgaben mit den jeweiligen Begründungen wurden wie folgt bewertet:

1 AES - Schlüsselaustausch II

Deine Antwort:

Keys: 1298074214633706907132624082304913; Keys per Party: 649037107316853453566312041152511

Deine Begründung:

Es muss insgesamt 2^110-111 Schlüssel benötigt werden. Es sei denn, jede von 110 Personen hat 2 Möglichkeiten: Schlüssel bekommen oder nicht. Daraus ergibt sich 2^110, aber wir müssen die 110 Fällen aussetzen wo nur 1 Person den Schlüssel hat, weil da keine Kommunikation stattfindet und den Fall, dass niemand Schlüssel bekommt. Daher ergibt sich 2^110-111

Für eine Person muss es 2^109-1 Schlüssel benötigt werden. Es sei denn, wenn er im Kommunikation steht, betrachten wir die restlichen Parteien. Jede von den restlichen Parteien hat im Prinzip 2 Möglichkeiten: entweder Schlussel besitzen oder nicht. Das führt zu 2^109 Schlüssel. Aber wir müssen den Fall wo alle anderen Parteien 0 Schlüssel besitzt. Daher ergibt sich 2^109-1

Bewertungsinformation:

Keine Anmerkungen

Erhaltende Punkte: 1 von 1

Letzter Abgabezeitpunkt: 2021-02-07 21:15:47

Aufgaben-Version: 695-2-80de21d2e246425e35091b8d655ab973

2 Access Control

Deine Antwort:

,rx,,,r,r,,,,,rwx,,-,-,,,wx,rw,,rw,,,,rw,,wx,,rwx,,w,,,w,rx,,,x,,,x,x,,,w,

Deine Begründung:

Wenn ein Benutzername zu einem File in der obigen Tabelle aufgelistet, dann tragen wir den

zugehorigen Zugriffsrecht in dem Matrix unten, ansonsten lassen wir die restlichen Felder leer

Bewertungsinformation:

Keine Anmerkungen

Erhaltende Punkte: 1 von 1

Letzter Abgabezeitpunkt: 2021-02-07 19:31:56

Aufgaben-Version: 863-2-35316e7396756a96573fc0c600aa9928

3 OneTimePad Hacking

Deine Antwort:

m1: YaoljHLV, m2: cf3lQffV, m3: VRaS7wIVzzm5bio9, k: 744e754e76664a49764d346d316b6858

Deine Begründung:

C1 XOR C2=(M1 XOR K) XOR (M2 XOR K)=M1 XOR K XOR M2 XOR K=(M1 XOR M2) XOR (K XOR K)=(M1 XOR M2) XOR 0=M1 XOR M2

Ich berechne die erste 8 Zeichen von M2 mit Hilfe von folgenden Formel

M1 XOR M2 XOR M1 = M2 => C1 XOR C2 XOR M1 = M2

Ich berechne die letzte 8 Zeichen von M1 mit Hilfe von folgenden Formel

M1 XOR M2 XOR M2 = M1 => C1 XOR C2 XOR M2 = M1

Ich berechne den Schluessel mit Hilfe von folgenden Formel

M1 XOR K=C1 => M1 XOR K XOR M1= K = C1 XOR M1

Ich berechne M3 mit Hilfe von folgenden Formel

M3 XOR K=C3 => M3 XOR K XOR K=M3=C3 XOR K

Bewertungsinformation:

Keine Anmerkungen

Erhaltende Punkte: 0 von 1

Letzter Abgabezeitpunkt: 2021-02-07 23:50:31

Aufgaben-Version: 628-2-c0e52f6c592bdcb07174bf5fbfad44fd

4 RSA - Schlüsselgenerierung

Deine Antwort:

N: 281857809097, Phi: 281856662676, E: 23, D: 36763912523

Deine Begründung:

n=p*q

phi(n)=(p-1)(q-1)

danach habe ich e=23 gewaehlt und dann habe ich mit Hilfe von meinem Erweiterter Euklidische Algorithmus auf Java d bestimmt.

```
public class GFG {
 public static void extendedEuclid(long a, long b, long[] d, long[] x, long[] y) {
        if (b == 0) {
            d[0] = a;
            x[0] = 1;
            y[0] = 0;
        } else {
            long[] x0 = new long[1];
            long[] y0 = new long[1];
            extendedEuclid(b, a % b, d, x0, y0);
            x[0] = y0[0];
            y[0] = x0[0] - a / b * y0[0];
        }
    }

    /*
     * Test code:
     *      Find a solution of a * x + b * y = c with given a, b, c.
     */
    public static void main(String[] args) throws IOException {



            long a = 23;
            long b = 281856662676L;
            long c =1;

            long[] d = new long[1];
            long[] x = new long[1];
```

long[] y = new long[1];

extendedEuclid(a, b, d, x, y);

(Begründung wurde bei 1000 Zeichen gekürzt)

Bewertungsinformation:

Keine Anmerkungen

Erhaltende Punkte: 1 von 1

Letzter Abgabezeitpunkt: 2021-02-07 23:57:01

Aufgaben-Version: 573-2-c2dea7ad5d2ff6ca045ee540b8433023

5 Path Traversal

Deine Antwort:

Path: ../../logs/ml46wexy.log

Deine Begründung:

Explanation not required

Bewertungsinformation:

Keine Anmerkungen

Erhaltende Punkte: 1 von 1

Letzter Abgabezeitpunkt: 2021-02-07 20:56:23

Aufgaben-Version: 352-2-15b430b27b9ad1ec1a264d67c20387dc

6 SQL Injection

Deine Antwort:

Not implemented for this task!

Deine Begründung:

Explanation not required

Bewertungsinformation:

Keine Anmerkungen

Erhaltende Punkte: 1 von 1

Letzter Abgabezeitpunkt: 2021-02-07 20:59:05

Aufgaben-Version: 352-2-457bc775c18ee1d5d235f2664ce37541

7 CBC Blockchiffre

Deine Antwort:

0001 0010 0011 1111

Deine Begründung:

Erster Klartextblock wird mit dem IV bitweise XOR Operationen zu 1000 durchgeführt, durch Verschlüsselungspermutation bekomme ich 0001, was ich bitweise XOR Operationen mit zweiten Klartextblock bearbeiten. Das Ergebnis davon ist 0100 und durch Verschlüsselungspermutation bekomme ich 0010. Die restliche Blöcke erfolgen analog dazu.

Bewertungsinformation:

Keine Anmerkungen

Erhaltende Punkte: 1 von 1

Letzter Abgabezeitpunkt: 2021-02-07 19:25:26

Aufgaben-Version: 462-2-4fd1ec103efd8a321e2422d5a552aff0

8 RSA - Signatur

Deine Antwort:

Signatur: 141259497758

Deine Begründung:

Ich berechne das Ergebnis mit Hilfe der Formel in der Vorlesung:

signsk(m)=(h(m)^d)mod n

Bewertungsinformation:

Keine Anmerkungen

Erhaltende Punkte: 1 von 1

Letzter Abgabezeitpunkt: 2021-02-07 23:52:02

Aufgaben-Version: 657-2-c3a025b80d2877d7e4eb9673b930fb27

9 Diffie-Hellman II

Deine Antwort:

A: 3, B: 15, K: 8;

Deine Begründung:

Das Ergebnis ergibt sich von folgenden Formeln

A=g^a mod p

B=g^b mod p

K=B^a mod p=A^b mod p

Bewertungsinformation:

Keine Anmerkungen

Erhaltende Punkte: 1 von 1

Letzter Abgabezeitpunkt: 2021-02-07 22:43:53

Aufgaben-Version: 572-2-12bcbd04a19cea71a55a0ba9aa4f29bf

10 Erw. Euklidischer Alg.

Deine Antwort:

X: 212, Y: -287

Deine Begründung:

Durch Faktorisierung bekomme ich 662=2*331 und 489=3*163 und daher ggT(662,489)=1

Nach Lemma von Bezout gibt es 2 ganze Zahlen x und y mit 662*x + 489*y=ggT(662, 489)=1, welche ich mit Hilfe von Erweiterter Euklidischer Algorithmus bestimmen kann.

Durch Erweiterter Euklidischer Algorithmus Berechnung bekomme ich a8=1, dieser Wert setze ich in Rückwerteinsetzenalgorithmus und bekomme am Ende a8=1=(212*a0-287*b0), also x ist 212 und y ist -287

Bewertungsinformation:

Keine Anmerkungen

Erhaltende Punkte: 1 von 1

Letzter Abgabezeitpunkt: 2021-02-07 19:15:14

Aufgaben-Version: 837-3-370b06d96824c5970c82db057b66ad79

11 Gesamtergebnis

Bei diesem Testat haben Sie 9 von 10 Punkten erreicht.