technische universität
dortmund

Sicherheit: Fragen und Lösungsansätze

Thomas Ruhroth

Übung 3

- HA1
- Antworten in Prüfungen
- Rückwärtsdenken

- Definitionen:
  - Kurz
  - Schnell
  - Präzise

Hausaufgaben

Hinweise zur Abgabe

- Stellen Sie die Lösung **präzise** und kurz dar
  - *Kurz* heißt nicht schluderig!
- Keine Email-Abgabe!
- Schreiben Sie nicht mehr Infos als nötig in die Lösungen
- Seien Sie eindeutig

- ✓ Richtig (kleinere Probleme werden ignoriert)
- ~ Überwiegend Richtig
  - Ungenauigkeit
  - Unrichtigkeit
  - Achten sie auf Unterstreichungen
- ¬ K „nicht knakig“
- NL nicht lesbar

PGP

- Viele (38) haben es erfolgreich geschafft
- 5x habe ich auch den Private Key bekommen
  - Mail mit Hinweis den Schlüssel zu revoken
- 2 mal wurde nur ein Teil der Nachricht (Nachricht oder Anhang) verschlüsselt.
- 1 mal wurde nicht mit meinem Key verschlüsselt
  - Kann die Mail dann nicht öffnen
- 1 mal wurde die Mail in einem ungültigem Format versandt

- Punkt:
  - 1 für den tauglichen Versuch
  - 1 für erfolgreiche Mail
  - 1 für erfolgreichen Anhang (Fingerprint ok und importrbar)

Pipi Langstrumpf

- 19 Abgaben haben es geschafft
- Häufigere Fehler:
  - Nicht vollständig bearbeitet
    - Insbesondere das Distributiv-Gesetz ist interessant, wurde aber fast nie betrachtet
    - Zwei Gruppen zu finden ist sehr einfach
  - Additive Element
    - x+y+2ist nicht mit dem Distributiv-Gesetz verträglich
- Einfache Idee: bestehenden Ring nehmen und Elemente umbenennen

Z/7Z mit 0->9, 2->6 und 6->2

+	9	1	6	3	4	5	2
9	9	1	6	3	4	5	2
1	1	6	3	4	5	2	9
6	6	3	4	5	2	9	1
3	3	4	5	2	9	1	6
4	4	5	2	9	1	6	3
5	5	2	9	1	6	3	4
2	2	9	1	6	3	4	5

*	9	1	6	3	4	5	2
9	9	9	9	9	9	9	9
1	9	1	6	3	4	5	2
6	9	6	4	2	1	3	5
3	9	3	2	6	5	1	4
4	9	4	1	5	6	2	3
5	9	5	3	1	2	4	6
2	9	2	5	4	3	6	1

Aufgabe 3

- $P = 4 = (0000\ 0100)_2 = (04)_{16}$
- $Q = 175 = (1010\ 1111)_2 = (AF)_{16}$
- $R = 90 = (0101\ 1010)_2 = (5a)_{16}$

- $P + Q = 171 = (1010\ 1011)_2 = (AB)_{16}$
- $P + R = 94 = (0101\ 1110)_2 = (5E)_{16}$
- $Q * 2 = 69 = (0100\ 0101)_2 = (45)_{16}$
- $R * (0B)_{16} = 8 = (0000\ 1000)_2 = (8)_{16}$

Mal und Plus mal anders

$$68_{16} \circ 3_{16} = 01101000_2 \circ 0000011_2$$

$$(x^6+x^5+x^3)*(x+1)\ mod\ (x^8+x^4+x^3+x+1)$$

$$(x^7+x^6+x^4+x^6+x^5+x^3)\ mod\ (x^8+x^4+x^3+x+1)$$

$$(x^7+x^4+x^5+x^3)\ mod\ (x^8+x^4+x^3+x+1)$$

$$(x^7+x^4+x^5+x^3)$$

$$10111000_2 = B8_{16}$$

Achtung: + ist XOR!

$$x^2+x^2=0 \qquad x^2+x^2+x^2=x^2$$

Definitionen

Zeit pro Definition 30 sec

Integrität

Assets

Objekt

Trust

Confidentiality

accountability

Security

authenticity

Schwache Kollisionsresistenz

Stromchiffre

Kerckhoffs-Prinzip

Starke Kollisionsresistenz

Stromchiffre

S-Box

Kryptoanalyse

privacy

Kryptographie

Schlüsselvereinbarung

One-Time-Pad

Steganographie

Safety

Faktorisierung

Message-Authentication-Code

Blockchiffre

Subjekte

Digitale Signature

Diskreter Logarithmus

Einwegfunktion

kryptographische Hashfunktion

Rückwärtsdenken

- Stoff wird in Vorlesungen linear dargestellt
- Aber Anwendung und Prüfungen sind nicht linear

Startaufgabe

- Stellen Sie sich vor sie müssten einen Übungszettel zu Signaturen erstellen.
- Was sind die Anforderungen die Sie in der Übungsaufgabe trainieren wollen würden:
  a) aus praktischer Sicht
  b) aus theoretischer Sicht

Lösung finden

- Erstellen Sie zu den Anforderungen aus der vorherigen Aufgabe ein Beispiel, welches die Lösung einer Übungsaufgabe darstellen könnte?

Aufgabe erstellen

- Erstellen Sie die Aufgabe