IT-Sec Tutorstunde 3

Carl Koenig, Fabian Specht

Vorstellung Hausaufgaben

- (7) XSS

(a) Kryptographie vs Krytpoanalyse

- Kryptographie

(a) Kryptographie vs Krytpoanalyse

- Kryptographie
  - Entwicklung sicherer Ver- und Entschluesselungsverfahren

(a) Kryptographie vs Krytpoanalyse

- Kryptographie
  - Entwicklung sicherer Ver- und Entschluesselungsverfahren
- Kryptoanalyse

(a) Kryptographie vs Krytpoanalyse

- Kryptographie
  - Entwicklung sicherer Ver- und Entschluesselungsverfahren
- Kryptoanalyse
  - Analyse von Verfahren mit dem Ziel, Schwachstellen zu finden

(b) Formen von Kryptographie

- symmetrisch

(b) Formen von Kryptographie

- symmetrisch
  - gleicher Schluessel fuer Ver- und Entschluesselung

(b) Formen von Kryptographie

- symmetrisch
  - gleicher Schluessel fuer Ver- und Entschluesselung
  - tendenziell effizienter

(b) Formen von Kryptographie

- symmetrisch
  - gleicher Schluessel fuer Ver- und Entschluesselung
  - tendenziell effizienter
- asymmetrisch

(b) Formen von Kryptographie

- symmetrisch
  - gleicher Schluessel fuer Ver- und Entschluesselung
  - tendenziell effizienter
- asymmetrisch
  - verschiedene Schluessel fuer Ver- und Entschluesselung

(b) Formen von Kryptographie

- symmetrisch
  - gleicher Schluessel fuer Ver- und Entschluesselung
  - tendenziell effizienter
- asymmetrisch
  - verschiedene Schluessel fuer Ver- und Entschluesselung
  - (pubkey, privkey)

(b) Formen von Kryptographie

- symmetrisch
  - gleicher Schluessel fuer Ver- und Entschluesselung
  - tendenziell effizienter
- asymmetrisch
  - verschiedene Schluessel fuer Ver- und Entschluesselung
  - (pubkey, privkey)
  - bspw. SSH u. PGP Email

(c) Kerckhoffs Prinzip

- Was ist das?

(c) Kerckhoffs Prinzip

- Was ist das?
  - Geheimhaltung eines Schluessels ist die **einzige** Grundlage fuer die Sicherheit eines Systems

(c) Kerckhoffs Prinzip

- Was ist das?
  - Geheimhaltung eines Schluessels ist die **einzige** Grundlage fuer die Sicherheit eines Systems
- Wann ist das sinnvoll?

(c) Kerckhoffs Prinzip

- Was ist das?
  - Geheimhaltung eines Schluessels ist die **einzige** Grundlage fuer die Sicherheit eines Systems
- Wann ist das sinnvoll?
  - immer! **No Security by Obscurity**

(d) Was ist ein gutes Verschluesselungsverfahren?

- Beispiel DES

(d) Was ist ein gutes Verschluesselungsverfahren?

- Beispiel DES
- Schluesselraum 2^56, 3 GHz, pro Instruktion wird ein Schluessel getestet. Wie lange brauchen wir mit Brute-Force?

(d) Was ist ein gutes Verschluesselungsverfahren?

- Beispiel DES
- Schluesselraum 2^56, 3 GHz, pro Instruktion wird ein Schluessel getestet. Wie lange brauchen wir mit Brute-Force?
  - 2^56 / 3 * 10^9 / 60 / 60 / 24 / 2 = 138.9

(d) Was ist ein gutes Verschluesselungsverfahren?

- Beispiel DES
- Schluesselraum 2^56, 3 GHz, pro Instruktion wird ein Schluessel getestet. Wie lange brauchen wir mit Brute-Force?
  - 2^56 / 3 * 10^9 / 60 / 60 / 24 / 2 = 138.9
  - COPA-COBANA schafft es in unter einer Woche [1]

[1] https://www.copacobana.org/

(e) Aber RSA Schluessel sind doch...

- deutlich komplexer, warum?

(e) Aber RSA Schluessel sind doch...

- deutlich komplexer, warum?
  - Analytische Verfahren auf RSA sind deutlich staerker

(3) Begriffe

- Konfusion

(3) Begriffe

- Konfusion
  - keine Beziehung zwischen Schluessel und aus Klartext generiertem Geheimtext

(3) Begriffe

- Konfusion
  - keine Beziehung zwischen Schluessel und aus Klartext generiertem Geheimtext
  - statische Kryptoanalyse ziehlt hierauf ab

(3) Begriffe

- Konfusion
  - keine Beziehung zwischen Schluessel und aus Klartext generiertem Geheimtext
  - statische Kryptoanalyse ziehlt hierauf ab
- Diffusion

(3) Begriffe

- Konfusion
  - keine Beziehung zwischen Schluessel und aus Klartext generiertem Geheimtext
  - statische Kryptoanalyse ziehlt hierauf ab
- Diffusion
  - Bits beeinflussen ganzen Datenblock

(4) RSA - Schluesselgenerierung

- waehle p, q prim

(4) RSA - Schluesselgenerierung

- waehle p, q prim
- n = p * q

(4) RSA - Schluesselgenerierung

- waehle p, q prim
- n = p * q
- phi(n) = (p - 1) * (q - 1)

(4) RSA - Schluesselgenerierung

- waehle p, q prim
- n = p * q
- phi(n) = (p - 1) * (q - 1)
- waehle e, sodass ggT(phi(n), e) = 1

(4) RSA - Schluesselgenerierung

- waehle p, q prim
- n = p * q
- phi(n) = (p - 1) * (q - 1)
- waehle e, sodass ggT(phi(n), e) = 1
- berechne d mit EEA

(4) RSA - Schluesselgenerierung

- waehle p, q prim
- n = p * q
- phi(n) = (p - 1) * (q - 1)
- waehle e, sodass ggT(phi(n), e) = 1
- berechne d mit EEA
- pub: (n, e)

(4) RSA - Schluesselgenerierung

- waehle p, q prim
- n = p * q
- phi(n) = (p - 1) * (q - 1)
- waehle e, sodass ggT(phi(n), e) = 1
- berechne d mit EEA
- pub: (n, e)
- priv: (p, q, d)

(4) RSA

- Klartext x, Chiffretext y

(4) RSA

- Klartext x, Chiffretext y
- Verschluesselung

(4) RSA

- Klartext x, Chiffretext y
- Verschluesselung
  - y = x^e mod N

(4) RSA

- Klartext x, Chiffretext y
- Verschluesselung
  - y = x^e mod N
- Entschluesselung

(4) RSA

- Klartext x, Chiffretext y
- Verschluesselung
  - y = x^e mod N
- Entschluesselung
  - x = y^d mod N