IT-Sec Tutorstunde 6

Carl Koenig, Fabian Specht

Vorstellung Hausaufgaben

- (13) TUMTime v2
- (15) Length Extension auf Keyed MACs

(1a) Encrypt-Then-MAC

- Warum ist Encrypt-Then-MAC gegenueber MAC-Then-Encrypt vorzuziehen?

(1a) Encrypt-Then-MAC

- Warum ist Encrypt-Then-MAC gegenueber MAC-Then-Encrypt vorzuziehen?
  - Denkt an Padding Oracle!

(1a) Encrypt-Then-MAC

- Warum ist Encrypt-Then-MAC gegenueber MAC-Then-Encrypt vorzuziehen?
  - Denkt an Padding Oracle!
- Problem: Bei Entschluesselung wird bereits mit Nachricht ohne Authentizitaet gearbeitet

(1a) Encrypt-Then-MAC

- Warum ist Encrypt-Then-MAC gegenueber MAC-Then-Encrypt vorzuziehen?
  - Denkt an Padding Oracle!
- Problem: Bei Entschluesselung wird bereits mit Nachricht ohne Authentizitaet gearbeitet
- fuehrte bei Padding Oracle dazu, dass Klartextinformationen geleakt wurden

(1b) AEAD

- Was sind Vorteile die AEAD gegenueber traditioneller, seperater Verschluesselung mit Integritaetsschutz via MAC

(1b) AEAD

- Was sind Vorteile die AEAD gegenueber traditioneller, seperater Verschluesselung mit Integritaetsschutz via MAC
  - benoetigt nur einen Schluessel

(1b) AEAD

- Was sind Vorteile die AEAD gegenueber traditioneller, seperater Verschluesselung mit Integritaetsschutz via MAC
  - benoetigt nur einen Schluessel
  - falsche Verwendung faellt schwieriger

(1c) Digitale Signaturen

- Was ist der Unterschied zwischen MACs und digitalen Signaturen?

(1c) Digitale Signaturen

- Was ist der Unterschied zwischen MACs und digitalen Signaturen?
  - asymm. <=> symm.

(1c) Digitale Signaturen

- Was ist der Unterschied zwischen MACs und digitalen Signaturen?
  - asymm. <=> symm.
  - eindeutige Identifikation <=> Teil irgendeiner Partei

(2a) PRNG

- wo werden PRNG eingesetzt?

(2a) PRNG

- wo werden PRNG eingesetzt?
  - Generierung von Schluesseln, Noncen, sicheres Padding etc.

(2b) PRNG Beispiel

```
def u32(x):
    return x & ((1 << 32) - 1)

def randgen_xorshift32 ():
    global state
    x = state
    x ^= u32(x << 13);
    x ^= u32(x >> 17);
    x ^= u32(x << 5);
    state = x
    return x
```

- berechne die ersten vier Zufallszahlen fuer Seed 1

(2c) PRNG Beispiel

- handelt es sich hier um einen CSPRNG?

(2c) PRNG Beispiel

- handelt es sich hier um einen CSPRNG?
  - Auf gar keinen Fall! Der interne Zustand wird immer ausgegeben

(2c) PRNG Beispiel

- handelt es sich hier um einen CSPRNG?
  - Auf gar keinen Fall! Der interne Zustand wird immer ausgegeben
  - niedrige Zahlen als Output lassen auf niedrigen verherigen Zustand schliessen

(2d) PRNG Beispiel

- wuerde es die Sicherheit verbessern, wenn nicht x, sondern x mod 16777217 zurueckgegeben wuerde?

(2d) PRNG Beispiel

- wuerde es die Sicherheit verbessern, wenn nicht x, sondern x mod 16777217 zurueckgegeben wuerde?
  - Nein! Falls kleiner als mod, wird immernoch der interne Zutand ausgegeben

(2d) PRNG Beispiel

- wuerde es die Sicherheit verbessern, wenn nicht x, sondern x mod 16777217 zurueckgegeben wuerde?
  - Nein! Falls kleiner als mod, wird immernoch der interne Zutand ausgegeben
  - Falls groesser, lassen sich moegliche interne Zustaende auf eine immer kleiner werdende Menge $\{x + 16777217, x + 2 * 16777217, \ldots\}$ runterbrechen

(3) Diffie-Hellman

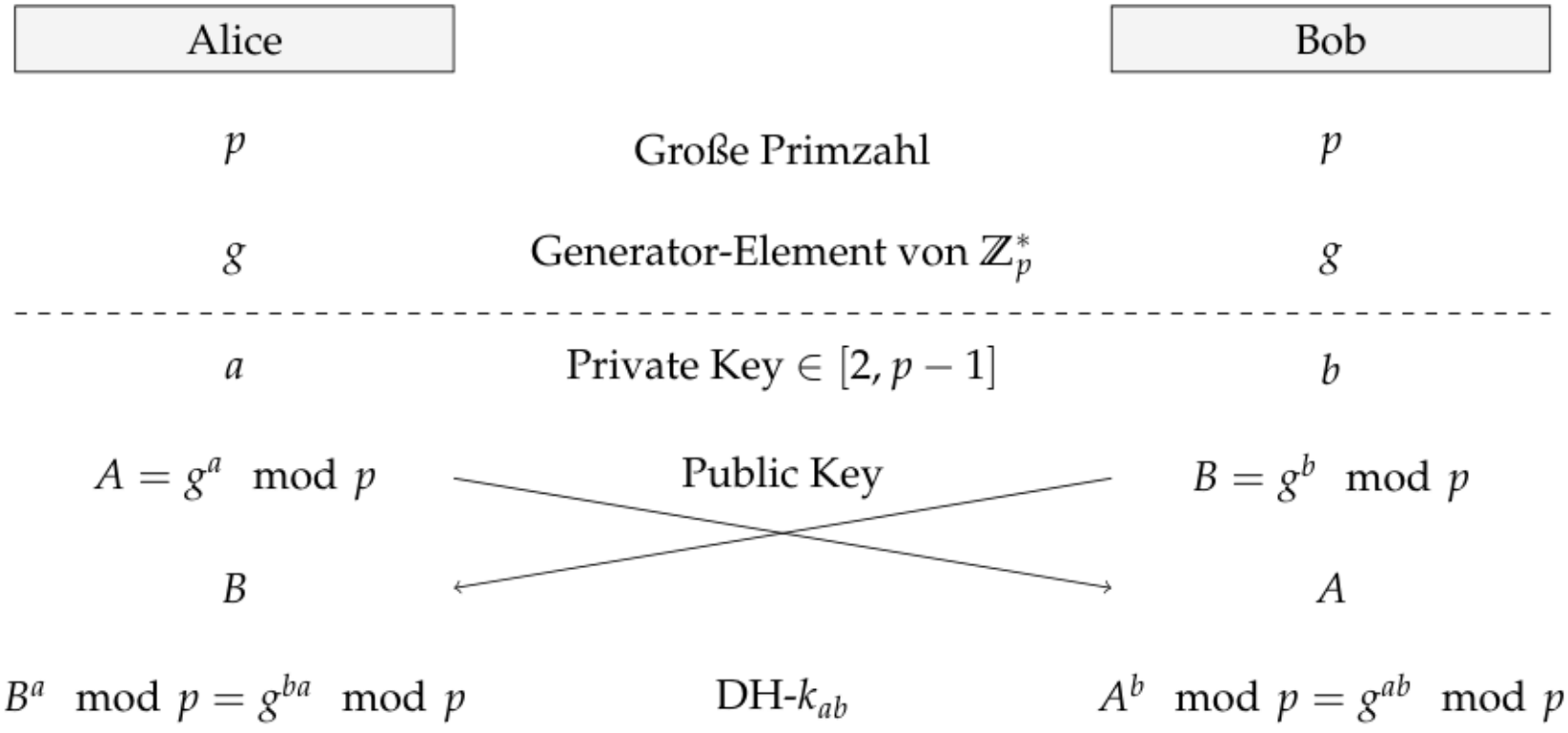

Figure 1: Textbook Diffie-Hellman

(3a) Diffie-Hellman

- probierts mal aus :)

(3b) Diffie-Hellman

- wie koennen wir nun aus diesem Integer einen AES Schluessel generieren?

(3b) Diffie-Hellman

- wie koennen wir nun aus diesem Integer einen AES Schluessel generieren?
- wird in Byte-Representation in sog. Key-Derivation-Function (KDF) eingefuegt, welche Digest beliebiger Laenge ausgibt

(3c) PFS

- was ist das?

(3c) PFS

- was ist das?
  - Knacken eines Schluessels soll niht die Sicherheit vergangener Kommunikation beeintraechtigen

(3c) PFS

- was ist das?
  - Knacken eines Schluessels soll niht die Sicherheit vergangener Kommunikation beeintraechtigen
  - Beispiel Diffie-Hellman: fuer jede neue Session wird ein neuer Schluessel generiert

(3d) PFS

- unter welchen Bedingungen gewaehrleistet ein DH-Schluesselaustausch PFS?

(3d) PFS

- unter welchen Bedingungen gewaehrleistet ein DH-Schluesselaustausch PFS?
  - auf beiden Seiten muessen immer frische private und oeffentliche Schluessel generiert werden - auch ephemeral DH genannt

(3d) PFS

- unter welchen Bedingungen gewaehrleistet ein DH-Schluesselaustausch PFS?
  - auf beiden Seiten muessen immer frische private und oeffentliche Schluessel generiert werden - auch ephemeral DH genannt
  - statischer DH wird allerdings gerne auf Chips mit geringer Rechenleisten verwendet