Kryptographie

Matheschülerzirkel Augsburg

12. April 2014

Der Heartbleed-Bug

Münzwurf über Telefon

- Kontext:
  Alice und Bob telefonieren.
  Sie müssen entscheiden, welcher von ihnen eine unliebsame Aufgabe übernimmt.

Münzwurf über Telefon

- Kontext:
  Alice und Bob telefonieren.
  Sie müssen entscheiden, welcher von ihnen eine unliebsame Aufgabe übernimmt.

1. Alice wählt Kopf, Bob wählt Zahl.
2. Alice wirft eine Münze.
3. Alice teilt Bob mit, dass die Münze Zahl anzeigt.
4. Bob muss die Aufgabe übernehmen.

Münzwurf über Telefon

- Kontext:
  Alice und Bob telefonieren.
  Sie müssen entscheiden, welcher von ihnen eine unliebsame Aufgabe übernimmt.

1. Alice wählt Kopf, Bob wählt Zahl.
2. Alice wirft eine Münze.
3. Alice teilt Bob mit, dass die Münze Zahl anzeigt.
4. Bob muss die Aufgabe übernehmen.

- Offensichtlich: Alice kann betrügen!

Münzwurf über Telefon (Forts.)

- Vereinfachung:
  Alice und Bob sitzen an einem Tisch.
  Sie müssen entscheiden, welcher von ihnen eine unliebsame Aufgabe übernimmt.

Münzwurf über Telefon (Forts.)

- Vereinfachung:
  Alice und Bob sitzen an einem Tisch.
  Sie müssen entscheiden, welcher von ihnen eine unliebsame Aufgabe übernimmt.

1. Alice nimmt eine Münze und legt sie unter eine Tasse. Bob weiß nicht, welche Seite nach oben zeigt.
2. Bob entscheidet sich für Kopf oder Zahl.
3. Alice deckt die Tasse auf.

Münzwurf über Telefon (Forts.)

- Vereinfachung:
  Alice und Bob sitzen an einem Tisch.
  Sie müssen entscheiden, welcher von ihnen eine unliebsame Aufgabe übernimmt.

1. Alice nimmt eine Münze und legt sie unter eine Tasse. Bob weiß nicht, welche Seite nach oben zeigt.
2. Bob entscheidet sich für Kopf oder Zahl.
3. Alice deckt die Tasse auf.

- Kein Zufall, Alice kontrolliert die Münze!
- Sicherheit durch gezwungene Festlegung

Einwegfunktionen

Definition

Eine Rechenvorschrift H heißt genau dann *Einwegfunktion*, wenn es sehr schwierig ist, zu gegebenem Funktionswert y eine Stelle x mit $H(x) = y$ zu finden.

- Beispiele: Name $\longmapsto$ Telefonnummer
  Text $\longmapsto$ SHA-256-Hash
- kein Beispiel: Buch $\longmapsto$ ISBN

- zusätzliche Forderung: Kollisionsresistenz

Digitale Imitation (unsichere Variante)

1. Alice entscheidet sich für Kopf (oder Zahl):
   $M :=$ `Münze zeigt Kopf`
2. Alice berechnet eine Einwegfunktion und teilt Bob das Ergebnis mit:
   $H(M) =$ `698eb5c9bcb789548188db9cc4`
3. Bob entscheidet sich für Kopf oder Zahl und teilt Alice seine Entscheidung mit.
4. Alice teilt Bob den Text M mit.
5. Bob berechnet seinerseits $H(M)$ und überprüft so Alice' Ergebnis.

Digitale Imitation (unsichere Variante)

1. Alice entscheidet sich für Kopf (oder Zahl):
   $M :=$ `Münze zeigt Kopf`
2. Alice berechnet eine Einwegfunktion und teilt Bob das Ergebnis mit:
   $H(M) =$ `698eb5c9bcb789548188db9cc4`
3. Bob entscheidet sich für Kopf oder Zahl und teilt Alice seine Entscheidung mit.
4. Alice teilt Bob den Text M mit.
5. Bob berechnet seinerseits $H(M)$ und überprüft so Alice' Ergebnis.

Digitale Imitation (unsichere Variante)

1. Alice entscheidet sich für Kopf (oder Zahl):
   $M :=$ `Münze zeigt Kopf`
2. Alice berechnet eine Einwegfunktion und teilt Bob das Ergebnis mit:
   $H(M) =$ `698eb5c9bcb789548188db9cc4`
3. Bob entscheidet sich für Kopf oder Zahl und teilt Alice seine Entscheidung mit.
4. Alice teilt Bob den Text M mit.
5. Bob berechnet seinerseits $H(M)$ und überprüft so Alice' Ergebnis.

Digitale Imitation (unsichere Variante)

1. Alice entscheidet sich für Kopf (oder Zahl):
   $M :=$ `Münze zeigt Kopf`
2. Alice berechnet eine Einwegfunktion und teilt Bob das Ergebnis mit:
   $H(M) =$ `698eb5c9bcb789548188db9cc4`
3. Bob entscheidet sich für Kopf oder Zahl und teilt Alice seine Entscheidung mit.
4. Alice teilt Bob den Text M mit.
5. Bob berechnet seinerseits $H(M)$ und überprüft so Alice' Ergebnis.

Digitale Imitation (unsichere Variante)

1. Alice entscheidet sich für Kopf (oder Zahl):
   $M :=$ `Münze zeigt Kopf`
2. Alice berechnet eine Einwegfunktion und teilt Bob das Ergebnis mit:
   $H(M) =$ `698eb5c9bcb789548188db9cc4`
3. Bob entscheidet sich für Kopf oder Zahl und teilt Alice seine Entscheidung mit.
4. Alice teilt Bob den Text M mit.
5. Bob berechnet seinerseits $H(M)$ und überprüft so Alice' Ergebnis.

Digitale Imitation (sichere Variante)

1. Alice entscheidet sich für Kopf (oder Zahl) und denkt sich ein Passwort aus:
   $M :=$ `GeheimesPasswort, Münze zeigt Kopf`
2. Alice berechnet eine Einwegfunktion und teilt Bob das Ergebnis mit:
   $H(M) =$ `ae30d422b3270dd66612c56637`
3. Bob entscheidet sich für Kopf oder Zahl und teilt Alice seine Entscheidung mit.
4. Alice teilt Bob den Text M mit.
5. Bob berechnet seinerseits $H(M)$ und überprüft so Alice' Ergebnis.

Digitale Imitation (sichere Variante)

1. Alice entscheidet sich für Kopf (oder Zahl) und denkt sich ein Passwort aus:
   $M :=$ `GeheimesPasswort, Münze zeigt Kopf`
2. Alice berechnet eine Einwegfunktion und teilt Bob das Ergebnis mit:
   $H(M) =$ `ae30d422b3270dd66612c56637`
3. Bob entscheidet sich für Kopf oder Zahl und teilt Alice seine Entscheidung mit.
4. Alice teilt Bob den Text M mit.
5. Bob berechnet seinerseits $H(M)$ und überprüft so Alice' Ergebnis.

Digitale Imitation (sichere Variante)

1. Alice entscheidet sich für Kopf (oder Zahl) und denkt sich ein Passwort aus:
   $M :=$ `GeheimesPasswort, Münze zeigt Kopf`
2. Alice berechnet eine Einwegfunktion und teilt Bob das Ergebnis mit:
   $H(M) =$ `ae30d422b3270dd66612c56637`
3. Bob entscheidet sich für Kopf oder Zahl und teilt Alice seine Entscheidung mit.
4. Alice teilt Bob den Text M mit.
5. Bob berechnet seinerseits $H(M)$ und überprüft so Alice' Ergebnis.

Digitale Imitation (sichere Variante)

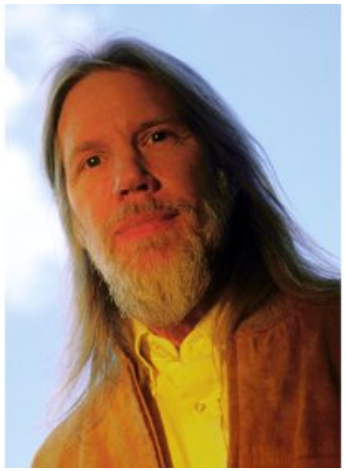
1. Alice entscheidet sich für Kopf (oder Zahl) und denkt sich ein Passwort aus:
   $M :=$ `GeheimesPasswort, Münze zeigt Kopf`
2. Alice berechnet eine Einwegfunktion und teilt Bob das Ergebnis mit:
   $H(M) =$ `ae30d422b3270dd66612c56637`
3. Bob entscheidet sich für Kopf oder Zahl und teilt Alice seine Entscheidung mit.
4. Alice teilt Bob den Text M mit.
5. Bob berechnet seinerseits $H(M)$ und überprüft so Alice' Ergebnis.

Digitale Imitation (sichere Variante)

1. Alice entscheidet sich für Kopf (oder Zahl) und denkt sich ein Passwort aus:
   $M :=$ `GeheimesPasswort, Münze zeigt Kopf`
2. Alice berechnet eine Einwegfunktion und teilt Bob das Ergebnis mit:
   $H(M) =$ `ae30d422b3270dd66612c56637`
3. Bob entscheidet sich für Kopf oder Zahl und teilt Alice seine Entscheidung mit.
4. Alice teilt Bob den Text M mit.
5. Bob berechnet seinerseits $H(M)$ und überprüft so Alice' Ergebnis.

Diffie–Hellman

- Kontext:
  Alice und Bob wollen ohne sonstige vorherige Absprachen ein gemeinsames Geheimnis ausmachen.



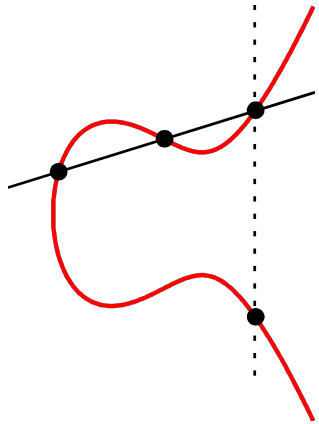
Diffie–Hellman (Forts.)

1. Fest: p Primzahl, g Primitivwurzel modulo p
2. Alice und Bob erzeugen je eine Zufallszahl, a bzw. b.
3. Alice $\to$ Bob: $A :\equiv g^a \mod p$
   Bob $\to$ Alice: $B :\equiv g^b \mod p$
4. Alice und Bob berechnen das Geheimnis:
   Alice: $K :\equiv B^a \mod p$
   Bob: $K :\equiv A^b \mod p$

- Gleiche Ergebnisse K!
- Worauf basiert die Sicherheit?
- Welche Schwachstelle hat das Verfahren?

Elliptische Kurven

- `http://en.wikipedia.org/wiki/Elliptic_curve`
- Dank der Gruppenstruktur kann man Diffie–Hellman auch mit elliptischen Kurven durchführen. Vorteil: Kürzere Schlüssellängen möglich, spannende Mathematik.
- Außerdem kann man Pseudozufallszahlen erzeugen (Tafel).
- Vermutlich hat die NSA in eine bestimmte Variante eine Hintertür eingebaut (Tafel).



Bildquellen

- http://biblioragazzi.files.wordpress.com/2008/04/reference.jpg
- http://i34.tinypic.com/51ptu0.jpg
- http://imgs.xkcd.com/comics/code_talkers.png
- http://one-time-pad.tripod.com/otp.jpg
- http://upload.wikimedia.org/wikipedia/commons/2/2b/Caesar3.svg
- http://www.bryx.de/wp-content/uploads/2008/09/800px-zeichen_220svg.png
- http://www.cellphones.ca/news/upload/2008/09/knowledge1.jpg
- http://www.digitaltrends.com/wp-content/uploads/2014/04/Heartbleed-bug.jpg
- http://www.gpuri.com/images/213/21325.jpg
- http://www.hirt-institut.de/de/Media/Shop/CategoryTextMedia/hirt_motiv_ihre_ziele.jpg
- http://www.hpl.hp.com/research/info_theory/images/curveplot.gif
- http://www.kveller.com/images/Article_images/wheres_waldo.jpg
- http://www.marketoracle.co.uk/images/coin-toss.jpg
- http://www.treachery.net/images/why_security_through_obscurity_isnt.jpg
- http://www.waleed-security.com/wp-content/uploads/2008/11/bruceab.jpg