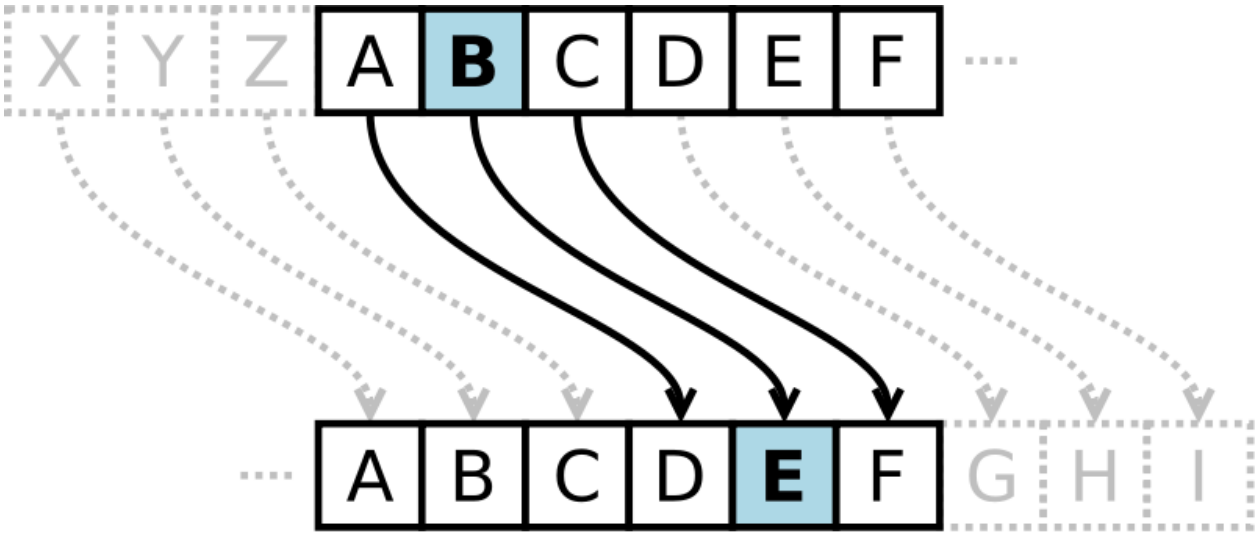
Hintergründe zur Kryptographie

Hanno Böck, http://www.hboeck.de/

3. Januar 2009


X Y Z A B C D E F
A B C D E F G H I

- Einfache Verschiebung des Alphabets
- Schlüsselraum: 26 Schlüssel
- Einfaches Beispiel für monoalphabetische Substitution

Beispiel: "DIES IST EIN TEXT", verschlüsselt mit "GEHEIM"

`DIESISTEINTEXT`

`GEHEIMGEHEIMGE`

`JMLWQEZIPRBQDX`

$D \Rightarrow 3,\ G \Rightarrow 6,\ D + G = 9,\ 9 \Rightarrow J$

$S \Rightarrow 18,\ M \Rightarrow 12,\ 18 + 12 = 30,\ 30\ \ mod\ \ 26 = 4,\ 4 \Rightarrow E$

- Symmetrisch: Schlüssel für Ver- und Entschlüsselung identisch (Beispiele: DES, AES, Twofish)
- $C = E(M, s)$; $M = D(C, s)$
- Asymmetrisch: Öffentlicher und privater Schlüssel (Beispiele: RSA, ElGamal, DSA)
- $C = E(M, pub)$; $M = D(C, priv)$

- Beide Partner einer Kommunikation, die keine Möglichkeit zum unbelauschten Kommunizieren haben, tauschen eine Reihe von Nachrichten aus und besitzen am Ende einen gemeinsamen Schlüssel
- Bekanntestes und einzig gängiges Verfahren: Diffie Hellmann

- Vorher gewählt und nicht geheim: große Primzahl p (bspw. 4096 Bit) und kleine Zahl g (Primitivwurzel)
- Alice wählt große Zufallszahl a, berechnet daraus $A = g^a \ mod \ p$ und sendet A an Bob
- Bob wählt große Zufallszahl b, berechnet daraus $B = g^b \ mod \ p$ und sendet B an Alice
- Alice berechnet B^a, Bob berechnet A^b
- $A^b = (g^a)^b \ mod \ p = (g^b)^a \ mod \ p = B^a$
- Alice und Bob besitzen gemeinsamen, geheimen Schlüssel
- Aus $g^a \ mod \ p$ (mit g, p bekannt) a zu berechnen: Diskreter Logarithmus, bei großen Zahlen schwer

- Einwegfunktion, die beliebige Eingabe auf Ausgabe fester länge projeziert
- Einfache Hashes: CRC32, Kryptographische Hashes: MD5, SHA1, SHA256
- Kryptographische Hashes: Aus dem Hash keine Information über Eingabe extrahierbar
- Erzeugen einer Kollission (zwei Eingaben mit identischem Hash) nicht mit vertretbarem Rechenaufwand erzeugbar

- Anwendungsbeispiel: Speicherung von Passwörtern (/etc/shadow)
- Passwort wird nicht gespeichert, sondern nur Hash des Passworts
- Wenn Hashes öffentlich werden, sind nicht automatisch Passwörter kompromittiert
- Wörterbuchangriffe und Rainbowtables

- 2004: Kollission bei MD5
- 2005/2006: Theoretische Angriffe auf SHA-1
- Im Moment: SHA-256, Zukunft: Wettbewerb des NIST

- Behandlung von Kryptographie als öffentliches Wissen vor 70er Jahren unüblich
- DES (Data Encryption Standard): Erstes standardisiertes Krypto-Verfahren (1976)
- Verfahren von IBM, Modifikationen der NSA
- Viel Raum für Verschwörungstheorien und Spekulationen
- NSA hatte wohl Kenntnisse, die in der öffentlichen Wissenschaft erst Jahre später bekannt wurden (Differentielle Kryptoanalyse)

- Wettbewerb des NIST
- 2000: Rijndael gewinnt AES-Wettbewerb
- 2002: Theoretischer Angriff gegen Rijndael (sehr theoretisch)
- Aus heutiger Sicht wäre Twofish vermutlich die bessere Wahl gewesen

- Alle gängigen Verfahren basieren entweder auf Faktorisierungsproblem oder auf diskretem Logarithmus
- Angriffe auf beide sehr ähnlich
- 512 Bit real gebrochen
- 1024 Bit in realistischer Reichweite, ist noch sehr häufig im Einsatz