## Selbststudium "Kryptographische Verfahren: Empfehlungen und Schlüssellängen"

Herausgeber: BSI: Bundesamt für Sicherheit in der Informationstechnik

Umfang: 78 Seiten

Zielpublikum: Entwickler die Systeme am 2016 entwickeln

jährliche Anpassung, beschränkt gültig bis Ende 2022

Annahme: keine kryptographisch relevante Anwendung von Quantencomputern

Sicherheitsniveau von mindetens 100-Bit (ideale Entropie)

Blockchiffren mit Blockgrösse >= 128-Bit 🡪 sonst zu häufiger Schlüsselwechsel nötig

Hashlänge mindestens 256-Bit

Inhalt:

1. Glossar
2. Einleitung
3. Symetrische Verschlüsselungsverfahren
   1. Empfohle Algorithmen für Blockchiffren: AES-128, AES-192, AES-256
   2. Betriebsarten:
      1. GCM: IV's dürfen niemals gleich sein
      2. CBC: Unvorhersagbare IV's verwenden
      3. CTR: Zählerstand darf sich nicht wiederholen
   3. Keine Algos für Streamciphern empfohlen, AES mit CBC erwähnt 🡪 Unbedingt Integrität der Daten schützen!
4. Asymmetrische Verschlüsselungsverfahren
   1. Emfolhene Verschlüsselungsferfahren
      1. ECIES(Elliptic Curve Integrated Encryption Scheme) mit 250-Bit Schlüssel
         1. MAC-Integriert
      2. DLIES(Discrete Logarithm Integrated Encryption Scheme) mit 2000-Bit Schlüssel(nach 2016 3000-Bit)
      3. RSA mit 2000-Bit Schlüssel(nach 2016 3000-Bit)
5. Hashfunktionen
   1. SHA-256, SHA-512/256, SHA-384 und SHA-512
   2. SHA3-256, SHA3-384, SHA3-512
   3. SHA-1 ist nicht mehr kollisionsresistent!
6. Datenauthentisierung
   1. Message Authentifaction Code (MAC)
      1. CMAC, HMAC, GMAC mit Schlüssel >= 16 Byte
   2. Signaturverfahren
      1. RSA
      2. DAS
         1. ECDSA
         2. ECKDSA, RCGDSA
      3. Merkle-Signaturen 🡪 Quantencomputer-Sicher, Forward-Secure
7. Instanzauthentisierung
   1. Wo mögliche gegenseitig
   2. Symetrische Verfahren
      1. Challene-Response 🡪 challenge minimum 100-Bit Entropie
         1. Response kann mit aus Kapitel 2 Algos erfolgen
   3. Asymmetrische Verfahren
      1. Wie symmetrisch, einfach mit Private/Public Keys und Signatur-Algo aus 5
   4. Passwortbasiert
      1. nach Möglichkeit Anzahl Versuche einschränken
      2. Minimale Passwort-Entropie von log2(10^6) 🡪 6-stellige PIN 🡪 Max 3 Versuche
      3. Nutzer auf PIN-Zufälligkeit sensibilisieren
8. Schlüsseleinigungsverfahren, Schlüsseltransportverfahren und Key-Update
   1. unbedingt Instanzauthentisierung
   2. beide Parner sollen gleichviel Anteil an neuem Schlüssel haben
   3. Symetrische Verfahren
      1. Transport: Verwendung von Algo aus Kap 2 🡪 Kombination mit MAC
   4. Asymmetrische Verfahren
      1. Diffie-Hellman verwendete Primzahl mindestens 2000-Bit lang
      2. EC Diffie-Hellman
      3. Implementierungfehler in beiden Verfahren weit verbreitet
9. Secret Sharing
   1. 4-Augen Prinzip bzw. t aus n Augen Prinzip 🡪 Aufteilung & Speicherung von Schlüsselinformationen
10. Zufallszahlengeneratoren
    1. Entropie von Seed muss mindestens so gross sein wie die im Kryptosystem verwendete Schlüssellängen
    2. Physikalische Zufallszahlengeneratoren
       1. Quelle muss überwacht werden 🡪 Bei Ausfall, defekt sofort abbrechen
       2. Experte beiziehen
    3. Deterministische Zufallszahlengeneratoren
       1. Vergangene/Zukünftige Werte sind nicht Rückschliessbar
       2. Auch wenn Innerer Zustand bekannt ist nach nächstem Reseed wieder ok
       3. Seed mittels Physikalischem Zufallszahlengenerator erzeugen bzw. Nicht-physikalisch nicht-deterministisch falls physikalisch nicht vorhanden
    4. Nicht-physikalische nicht-deterministische Zufallszahlengeneratoren
       1. Nutzen Systemressourcen(RAM, Systemzeit, …), Benutzereingaben 🡪 /dev/random
    5. Seedgenerierung
       1. Linux: /dev/random
       2. Windows: Kombination von ReadTimeStampCounter() und GetSystemTimeAsfileTime() 🡪 unabhängig und möglichst unvorhersehbar und mit Mitwirkung des Users aufrufen
11. Anhang A Anwendung kryptografische Verfahren
    1. Verschlüsselung mit Datenauthentifizierung(Secure Messaging)
       1. Kombination aus Kap 2 und 5 MAC's
          1. nur verschlüsselte Daten authentifizieren und ggf. nicht verschlüsselte nicht vertrauliche Daten
          2. Verschlüsselungs-Schlüssel != Authentifizierungs-Schlüssel und keiner aus anderem ableitbar. wenn dann werden beide von einem gemeinsamen Schlüssel abgeleitet
    2. Authentisierte Schlüsselvereinbarung
       1. mit Instanzauthentifizieerung kombinieren
12. Anhang B Zusätzliche Funktionen und Algorithmen
    1. Schlüsselableitung
       1. Key Derivation through Extraction-then-Expansion in Kombo mit geeignetem MAC
    2. Unvorhersagbare IV's für CBC erzeugen
       1. Zufälliger, genügend Entropie IV
       2. mittels deterministischem Verfahren, z.B. Counter Prä-IV, und diesen mittels der einzusetztenden Block-chifffre und schlüssel verschlüsseln 🡪 Counter darf sich niemals wiederholen
    3. Erzeugung von EV-Systemparametern
       1. nicht selbst erzeugen sondern auf vertrauenswürdige Quellen zurückgreiffen
    4. Generierung von Zufallszahlen für probabilistische asymmetrische Verfahren
    5. Probabilistische Primzahltests
       1. Miller-Rabin Primzahltest verwenden
13. Anhang C Protokolle für spezielle kryptografische Anwendungen
    1. SRTP, spezielle, weniger strikte Anforderungen da System sehr performat/zeitkritisch sein muss