

Skydd för känsliga data

Daniel Bosk¹

Avdelningen för informations- och kommunikationssystem (IKS),
Mittuniversitetet, Sundsvall.

data.tex 1325 2013-09-23 19:29:21Z danbos

¹Detta verk är tillgängliggjort under licensen Creative Commons Erkännande-DelaLika 2.5 Sverige (CC BY-SA 2.5 SE). För att se en sammanfattning och kopia av licenstexten besök URL

<http://creativecommons.org/licenses/by-sa/2.5/se/>

Översikt

- 1 **Introduktion**
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Översikt

- 1 Introduktion
 - **Kryptosystem**
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

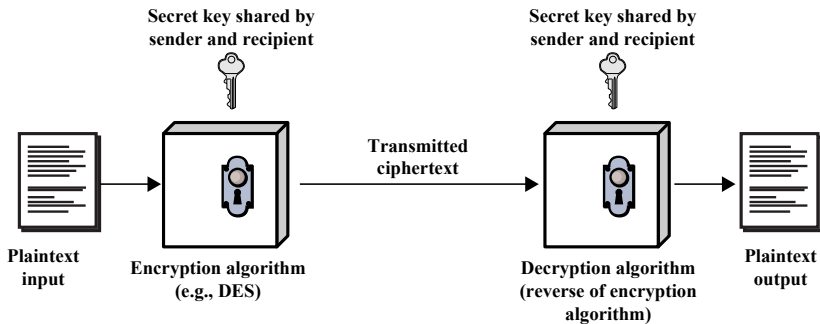
Kryptosystem

- Ordet kryptografi kommer från grekiskans κρυπτός (*kryptos*) och γράφος (*graphos*) [13b].
- Dessa betyder *gömd* eller *hemlig* [13a] respektive *skrift* [13c].
- Ordet kryptografi betyder följaktligen *hemlig skrift*.
- I modern tid är kryptografin ett högst matematiskt område.
- Det finns inte utrymme för annat än matematisk precision.

Kryptosystem

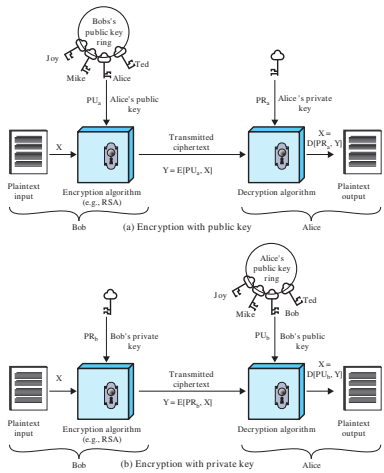
- Autentisering (authentication).
- Oförnekelsebarhet (non-repudiation).
- Konfidentialitet (confidentiality).
- Riktighet (integrity).

Kryptosystem



Figur : Översikt av symmetrisk kryptering. Bild: [Sta11].

Kryptosystem



Figur : Översikt av asymmetrisk kryptering. Bild: [Sta11].

Kryptosystem

Definition

Ett *kryptosystem* är en tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ där följande gäller:

- ① \mathcal{P} är en ändlig mängd av möjliga klartexter.
- ② \mathcal{C} är en ändlig mängd av möjliga kryptotexter.
- ③ \mathcal{K} , kallad *nyckelrymden*, är en ändlig mängd av möjliga nycklar.
- ④ För varje $k \in \mathcal{K}$ finns en *krypteringsregel* $e_k \in \mathcal{E}$ och motsvarande *avkrypteringsregel* $d_k \in \mathcal{D}$. Varje $e_k: \mathcal{P} \rightarrow \mathcal{C}$ och $d_k: \mathcal{C} \rightarrow \mathcal{P}$ är funktioner sådana att $d_k(e_k(p)) = p$ för alla klartexter $p \in \mathcal{P}$.

Kryptosystem

- Typer av operationer för att transformera klartext till kryptotext.
- Antalet nycklar som används.
- Sätt att processa klartexten:
 - Blockchiffer.
 - Strömchiffer.

Kryptosystem

Kryptanalys

- Enbart chiffrtext (ciphertext only).
- Känd klartext (known plaintext).
- Vald klartext (chosen plaintext).
- Vald kryptotext (chosen ciphertext).
- Vald text (chosen text).

Kryptosystem

Definition

Ett kryptosystem är beräkningsmässigt säkert om det uppfyller någon eller båda av följande:

- Kostnaden för att knäcka chiffret är högre än värdet på informationen det skyddar.
- Tiden det tar att knäcka chiffret är längre än tiden informationen är värdefull.

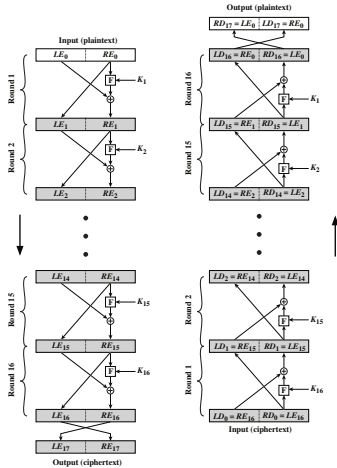
Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Översikt

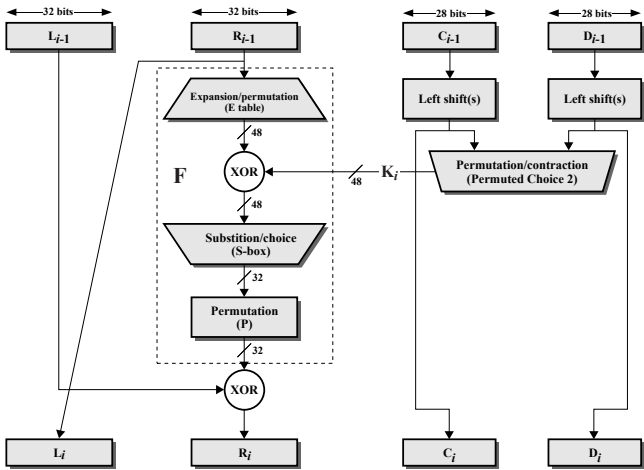
- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - **Data Encryption Standard (DES)**
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Data Encryption Standard (DES)



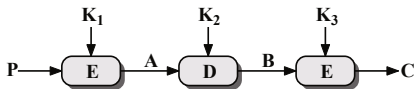
Figur : Feistelstruktur. Bild: [Sta11].

Data Encryption Standard (DES)

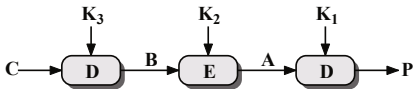


Figur : En runda i DES. Bild: [Sta11].

Data Encryption Standard (DES)



(a) Encryption



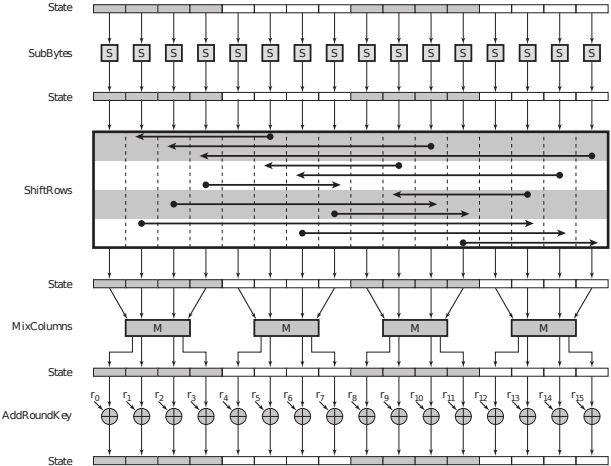
(b) Decryption

Figur : DES tillämpad i 3DES. Bild: [Sta11].

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - **Advanced Encryption Standard (AES)**
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Advanced Encryption Standard (AES)



Figur : En runda i AES. Bild: [Sta11].

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 **Pseudoslumptal och strömchiffer**
 - **Pseudoslumptal**
 - **Strömchiffer**
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - **Pseudoslumptal**
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Pseudoslumptal

- Pseudorandom number generator.
- True random number generator.
- Pseudorandom function.

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - **Strömchiffer**
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Strömchiffer

- Pseudorandom number generator som utgår från nyckeln.

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 **Block Modes of Operation**
 - **Introduktion**
 - **Några andra modes of operation**
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - **Introduktion**
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Introduktion

- Ett blockchiffer i standardutförande är inte särskilt säkert om vi vill kryptera mer än ett block med samma nyckel.
- För att åtgärda detta använder vi olika "modes of operation" för blockchiffer.

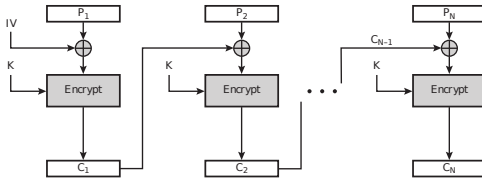
Introduktion

- Det enklaste är "electronic code-book mode" (ECB).
- Detta går ut på att vi delar upp meddelandet enligt blockstorleken och krypterar del för del.

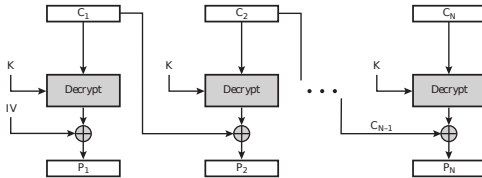
Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - **Några andra modes of operation**
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Några andra modes of operation



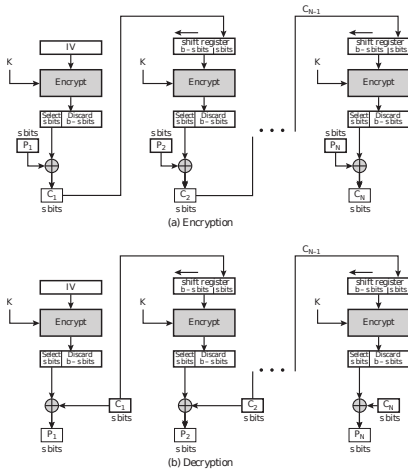
(a) Encryption



(b) Decryption

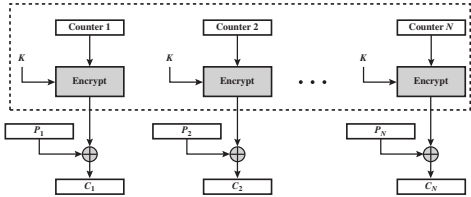
Figur : Cipher block chaining (CBC) mode. Bild: [Sta11].

Några andra modes of operation

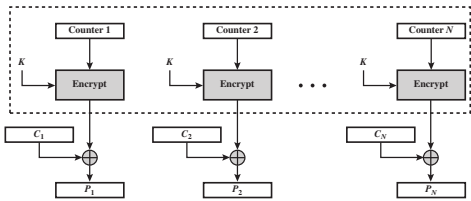


Figur : Cipher feedback (CFB) mode. Bild: [Sta11].

Några andra modes of operation



(a) Encryption



(b) Decryption

Figur : Counter (CTR) mode. Bild: [Sta11].

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 **Moderna asymmetriska chiffer**
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - **RSA**
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

RSA

Sats (Fermat–Eulers sats)

Om n och a är heltal sådana att $\gcd(n, a) = 1$, då gäller att $a^{\phi(n)} \equiv 1 \pmod{n}$.

RSA

Rivest, Shamir, Adleman (RSA)

Definition

Låt $n = pq$, där p och q är primtal. Låt $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$ och

$$\mathcal{K} = \{(n, p, q, e, d) : ed \equiv 1 \pmod{\phi(n)}\}.$$

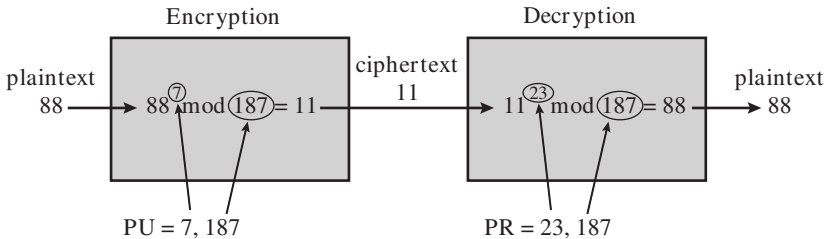
För $k = (n, p, q, e, d)$ definiera

$$e_k(p) = p^e \pmod{n} \text{ och}$$

$$d_k(c) = c^d \pmod{n},$$

där $p \in \mathcal{P}$ och $c \in \mathcal{C}$. Tupeln (n, e) utgör den *publika nyckeln* och (p, q, d) den *privata nyckeln*.

RSA

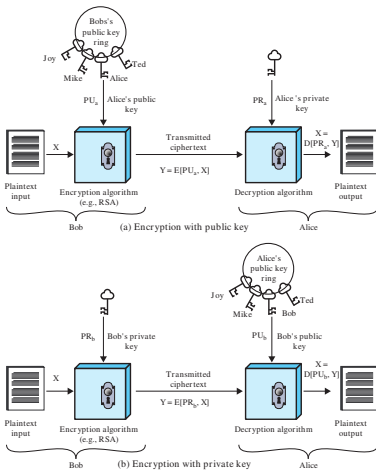


Figur : Ett exempel på kryptering med RSA. Bild: [Sta11].

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - **Digitala signaturer**
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Digitala signaturer



Figur : Översikt av asymmetrisk kryptering. Bild: [Sta11].

Digitala signaturer

Kryptering $E_{k_A}(m) = c \longrightarrow D_{k_A}(c) = E_{k_A^{-1}}(c) = m$

Signering $D_{k_A}(m) = E_{k_A^{-1}}(m) = c \longrightarrow E_{k_A}(c) = m$

Digitala signaturer

- Kan ha digitala signaturer med symmetriska chiffer, men i mycket begränsad utsträckning.
- Det är inte jag som skapat detta meddelande, då måste det vara den andre.
 - A och B delar nyckeln k .
 - A tar emot n , $E_k(n, m)$.
 - A vet att A inte skapat meddelandet, alltså måste någon annan med tillgång till nyckeln k gjort det.
 - Eftersom att B är den enda utöver A som känner till nyckeln måste meddelandet m vara från B .

Översikt

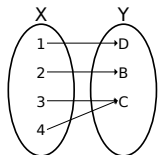
- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 **Hashfunktioner**
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Översikt

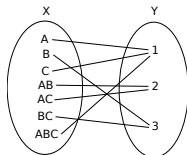
- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - **Introduktion till hashfunktioner**
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Introduktion till hashfunktioner

- En hashfunktion är en funktion $h: X \rightarrow Y$, där X är en möjligen oändlig mängd och Y är en ändlig mängd.
- Den är således en icke-injektiv surjektiv funktion och saknar invers $h^{-1}: Y \rightarrow X$ sådan att $h^{-1}(h(x)) = x$ för alla $x \in X$.



(a)
 $h: X \rightarrow Y$



(b) $h': X \rightarrow Y$

Figur : Två icke-injektiva surjektiva funktioner h respektive h' .

Introduktion till hashfunktioner

- Finns många olika hashfunktioner:
 - MD5,
 - SHA1,
 - SHA256,
 - SHA512.
- Tillämpningsområdet är stort:
 - verifiera integritet hos filer,
 - snabb sökning i datastrukturer,
 - digitala signaturer,
 - skydda lösenord.

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - **Formell behandling av hashfunktioner**
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Formell behandling av hashfunktioner

Definition

En *hashfamilj* är en tupel $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{H})$, där

- \mathcal{X} är mängden av möjliga *meddelanden*.
- \mathcal{Y} är en ändlig mängd av möjliga *meddelandesammandrag*.
- \mathcal{K} är en ändlig mängd av möjliga nycklar.
- För varje nyckel $k \in \mathcal{K}$ finns en hashfunktion $h_k \in \mathcal{H}$ sådan att $h_k: \mathcal{X} \rightarrow \mathcal{Y}$.

Formell behandling av hashfunktioner

- \mathcal{X} kan vara ändlig eller oändlig, men alltid $|\mathcal{X}| \geq |\mathcal{Y}|$.
- Vissa hashfunktioner saknar nycklar, då är $|\mathcal{K}| = 1$.
- Låt $\mathcal{Y}^{\mathcal{X}}$ beteckna mängden av alla funktioner från \mathcal{X} till \mathcal{Y} , då är $|\mathcal{Y}^{\mathcal{X}}| = |\mathcal{Y}|^{|\mathcal{X}|}$.

Formell behandling av hashfunktioner

Preimage resistant eller one-way

Inversa bilden (*preimage*)

- ① Given hashfunktionen $h: \mathcal{X} \rightarrow \mathcal{Y}$ och element $y \in \mathcal{Y}$.
- ② Hitta $x \in \mathcal{X}$ sådant att $h(x) = y$.

Formell behandling av hashfunktioner

Second preimage resistant

Andra inversa förbilden (*second preimage*)

- ① Given hashfunktionen $h: \mathcal{X} \rightarrow \mathcal{Y}$ och element $x \in \mathcal{X}$.
- ② Hitta $x' \in \mathcal{X}$ sådant att $x' \neq x$ och $h(x') = h(x)$.

Formell behandling av hashfunktioner

Collision resistant

Kollision

- ① Given hashfunktionen $h: \mathcal{X} \rightarrow \mathcal{Y}$.
- ② Hitta $x, x' \in \mathcal{X}$ sådana att $x' \neq x$ och $h(x') = h(x)$.

Formell behandling av hashfunktioner

Random Oracle Model

- Idealisering av en hashfunktion.
- Kan liknas vid ett orakel som ger slumpmässiga svar på frågor.
- Men vid upprepningar ska samma svar ges.
- En funktion $h \in \mathcal{Y}^{\mathcal{X}}$ väljs slumpmässigt, vi får enbart ställa frågor som "vad är $h(x)$?"
- Innan vi ställer frågan $h(x)$ vet vi ingenting om h .
- Efter att vi ställt frågan $h(x)$ och erhållit svaret y , då vet vi enbart att $h(x) = y$.

Formell behandling av hashfunktioner

- Det går att visa att om man kan hitta en andra invers avbildning, då kan man hitta en kollision.
- Det går även att visa att om man kan hitta en invers avbildning, då kan man hitta en kollision.
- Följaktligen, om en hashfunktion är *collision resistant*, då är den även *preimage* och *second preimage resistant*.

Formell behandling av hashfunktioner

- Vi kan visa att för att ha 50 procent sannolikhet att hitta en kollision krävs $Q \approx 1.17\sqrt{|\mathcal{Y}|}$ antal gissningar.
- Detta kallas födelsedagsparadoxen.
- Detta betyder att om $|\mathcal{Y}| = 365$, då är den 50 % sannolikhet att kollisionsalgoritmen finner en kollision då $Q = 23$.
- Om en fingeravtrycksläsare lagrar fingeravtryck som 20 bitar långa bitsträngar, då är det 50 % sannolikhet att två personer kan identifiera sig som varandra vid 1000 användare.
- Vi kan finna kollisioner med 50 % sannolikhet för en hashfunktion som har 256 bitars meddelandesammandrag med 2^{128} gissningar.

Formell behandling av hashfunktioner

MD5 Fullständigt knäckt; kan finna godtyckliga kollisioner, snabb att beräkna [se LD05].

SHA1 Finns attacker som antyder att det går att finna kollisioner med $Q = 2^{69}$, borde vara $Q = 2^{80}$.

SHA256 Inga attacker som är märkbart lägre än $Q = 2^{128}$.

SHA512 Inga attacker som är märkbart lägre än $Q = 2^{256}$.

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 **Meddelandeautentisering**
 - **Message Authentication Code (MAC)**
 - **Hashfunktionsbaserade MAC**
 - **MAC baserade på blockchiffer**
 - **Chiffer med autentisering**

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - **Message Authentication Code (MAC)**
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

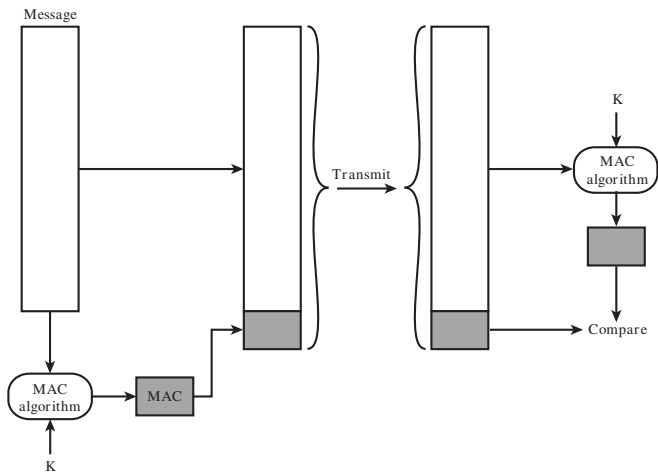
Message Authentication Code (MAC)

- Vi har sett att både symmetrisk och asymmetrisk kryptering kan användas för att signera kod.
- Dock uppstår problem om vi använder exempelvis ECB som mode of operation.
 - Byt ordning på blocken.
 - Ta bort vissa block.
- För detta ändamål skapar vi MAC.

Översikt

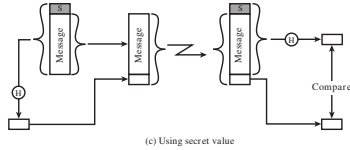
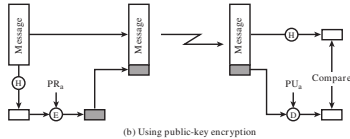
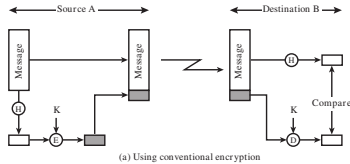
- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - **Hashfunktionsbaserade MAC**
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Hashfunktionsbaserade MAC



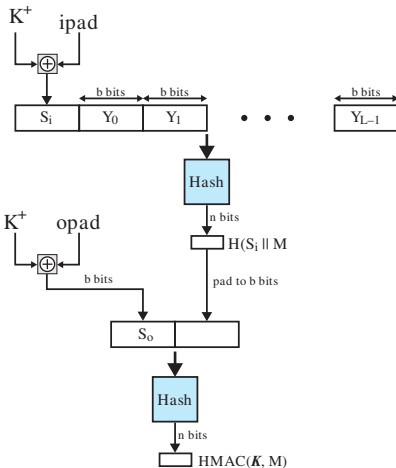
Figur : En översikt av en enkel MAC. Bild: [Sta13].

Hashfunktionsbaserade MAC



Figur : Exempel på olika former av MAC. Bild: [Sta13].

Hashfunktionsbaserade MAC



Figur : Hashbaserad MAC kallad HMAC,
 $HMAC(K, M) = h[(K^+ \oplus opad) || h[(K^+ \oplus ipad) || M]]$. Bild: [Sta13].

Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - **MAC baserade på blockchiffer**
 - Chiffer med autentisering

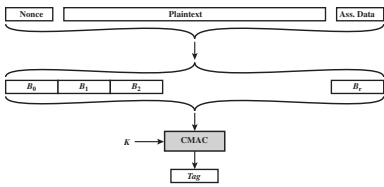
Översikt

- 1 Introduktion
 - Kryptosystem
- 2 Moderna symmetriska chiffer
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
- 3 Pseudoslumptal och strömchiffer
 - Pseudoslumptal
 - Strömchiffer
- 4 Block Modes of Operation
 - Introduktion
 - Några andra modes of operation
- 5 Moderna asymmetriska chiffer
 - RSA
 - Digitala signaturer
- 6 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 7 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - **Chiffer med autentisering**

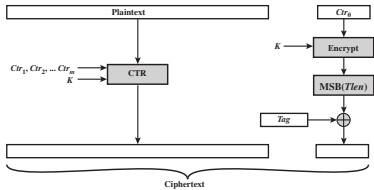
Chiffer med autentisering

- Counter with Cipher Block Chaining Message Authentication Code (CCM).
- Är ett mode of operation för kryptering med autentisering.

Chiffer med autentisering



(a) Authentication



(b) Encryption

Figur : En schematisk översikt av CCM. Bild: [Sta13].

Referenser



“crypto-, comb. form”. I: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, mars 2013. URL: <http://www.oed.com/view/Entry/45363>.



“cryptography, n.” I: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, mars 2013. URL: <http://www.oed.com/view/Entry/45374?redirectedFrom=cryptography&>.



“graphy-, comb. form”. I: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, mars 2013. URL: <http://www.oed.com/view/Entry/80855>.



Stefan Lucks och Magnus Daum. *Hash Collisions (The Poisoned Message Attack)*. 2005. URL: <http://th.informatik.uni-mannheim.de/people/lucks/HashCollisions/>.



William Stallings. *Cryptography and network security : principles and practice*. 5. ed. International ed. Upper