


Asymmetrisk kryptografi och meddelandeautentisering

Daniel Bosk¹

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

pubkey.tex 1314 2013-09-20 17:57:20Z 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 Asymmetrisk kryptografi
 - Introduktion
 - Kryptosystem
 - Digitala signaturer
- 2 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 3 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Litteratur

The lecture covers chapter 3 “Public-Key Cryptography and Message Authentication” in [Sta13] and the remaining parts of chapter 5 “Cryptography” in [And08].

After this you should solve problems 3.1, 3.2, 3.5, 3.7, 3.8, 3.9 and 3.10 in [Sta13].

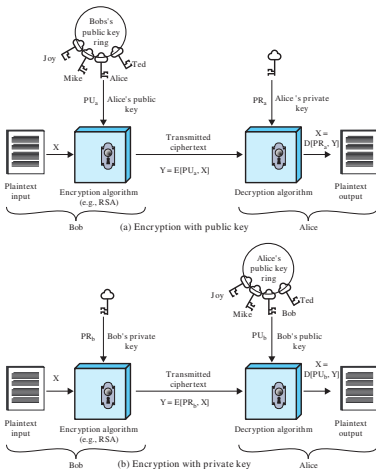
Översikt

- 1 Asymmetrisk kryptografi
 - Introduktion
 - Kryptosystem
 - Digitala signaturer
- 2 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 3 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Översikt

- 1 Asymmetrisk kryptografi
 - **Introduktion**
 - Kryptosystem
 - Digitala signaturer
- 2 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 3 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Introduktion



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

Introduktion

Sats (Fermat–Eulers sats)

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

Översikt

- 1 Asymmetrisk kryptografi
 - Introduktion
 - **Kryptosystem**
 - Digitala signaturer
- 2 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 3 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Kryptosystem

Rivest, Shamir, Adleman (RSA)

Definition

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

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

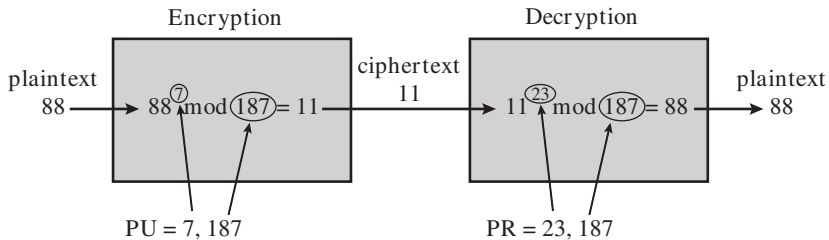
För $k = (n, p, q, e, d)$ definiera

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

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

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

Kryptosystem

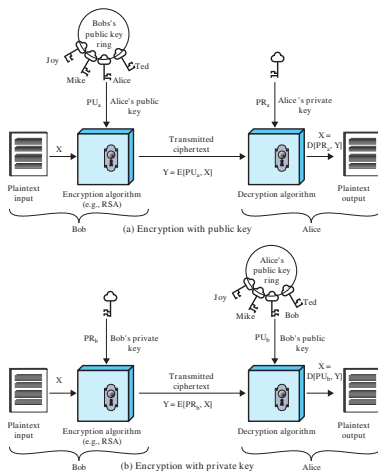


Figur : Ett exempel på kryptering med RSA. Bild: [Sta11].

Översikt

- 1 Asymmetrisk kryptografi
 - Introduktion
 - Kryptosystem
 - Digitala signaturer
- 2 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 3 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

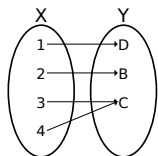
- 1 Asymmetrisk kryptografi
 - Introduktion
 - Kryptosystem
 - Digitala signaturer
- 2 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 3 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Översikt

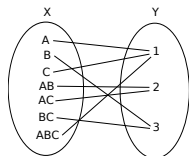
- 1 Asymmetrisk kryptografi
 - Introduktion
 - Kryptosystem
 - Digitala signaturer
- 2 Hashfunktioner
 - **Introduktion till hashfunktioner**
 - Formell behandling av hashfunktioner
- 3 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - 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 Asymmetrisk kryptografi
 - Introduktion
 - Kryptosystem
 - Digitala signaturer
- 2 Hashfunktioner
 - Introduktion till hashfunktioner
 - **Formell behandling av hashfunktioner**
- 3 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

Sats (Oberoendesatsen)

Antag att $h \in \mathcal{Y}^{\mathcal{X}}$ väljs slumpmässigt. Låt $\mathcal{X}_0 \subseteq \mathcal{X}$. Antag att värdet $h(x)$ bestäms genom att fråga oraklet om och endast om $x \in \mathcal{X}_0$. Då gäller att

$$\Pr(h(x) = y) = \frac{1}{|\mathcal{Y}|}$$

för alla $x \in \mathcal{X} \setminus \mathcal{X}_0$ och alla $y \in \mathcal{Y}$.

Formell behandling av hashfunktioner

Algorithm (Hitta invers avbild)

input $h \in \mathcal{Y}^{\mathcal{X}}, y \in \mathcal{Y}, Q \in \mathbb{N}$

output x sådant att $h(x) = y$

Välj någon mängd $\mathcal{X}_0 \subseteq \mathcal{X}$ sådan att $|\mathcal{X}_0| = Q$.

for all $x \in \mathcal{X}_0$ **do**

if $h(x) = y$ **then**

return x

end if

end for

return misslyckande

Formell behandling av hashfunktioner

Sats

För någon mängd $\mathcal{X}_0 \subseteq \mathcal{X}$ med $|\mathcal{X}_0| = Q$ är sannolikheten ϵ att algoritmen för att finna en inverterad avbildning lyckas

$$\epsilon = 1 - \left(1 - \frac{1}{|\mathcal{Y}|}\right)^Q.$$

Formell behandling av hashfunktioner

Algorithm (Hitta kollision)

input $h \in \mathcal{Y}^{\mathcal{X}}, Q \in \mathbb{N}$

output $x, x' \in \mathcal{X}$ sådana att $x \neq x', h(x) = h(x')$

Välj någon mängd $\mathcal{X}_0 \subseteq \mathcal{X}$ sådan att $|\mathcal{X}_0| = Q$.

for all $x \in \mathcal{X}$ **do**

 Låt $y_x = h(x)$.

end for

if $y_x = y_{x'}$ för något $x \neq x'$ **then**

return (x, x')

end if

return misslyckande

Formell behandling av hashfunktioner

Sats

För någon mängd $\mathcal{X}_0 \subseteq \mathcal{X}$ med $|\mathcal{X}_0| = Q$ är sannolikheten ϵ för att kollisionsalgoritmen lyckas följande:

$$\epsilon = 1 - \left(\frac{|\mathcal{Y}| - 1}{|\mathcal{Y}|} \right) \left(\frac{|\mathcal{Y}| - 2}{|\mathcal{Y}|} \right) \cdots \left(\frac{|\mathcal{Y}| - Q + 1}{|\mathcal{Y}|} \right).$$

Formell behandling av hashfunktioner

- Vi hade att sannolikheten för ingen kollision är $\prod_{i=1}^{Q-1} (1 - 1/|\mathcal{Y}|)$.
- För små x gäller att $1 - x \approx e^{-x}$.
- Då får vi

$$\prod_{i=1}^{Q-1} (1 - 1/|\mathcal{Y}|) \approx \prod_{i=1}^{Q-1} e^{-i/|\mathcal{Y}|} = e^{-\sum_{i=1}^{Q-1} i/|\mathcal{Y}|}.$$

- Följaktligen gäller $e^{-\sum_{i=1}^{Q-1} i/|\mathcal{Y}|} \approx 1 - \epsilon$.
- Med lite omskrivningar får vi $Q \approx \sqrt{2|\mathcal{Y}| \log \frac{1}{1-\epsilon}}$.
- För $\epsilon = 1/2$ får vi då $Q \approx 1.17\sqrt{|\mathcal{Y}|}$.

Formell behandling av hashfunktioner

- 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 Asymmetrisk kryptografi
 - Introduktion
 - Kryptosystem
 - Digitala signaturer

- 2 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner

- 3 Meddelandeautentisering
 - **Message Authentication Code (MAC)**
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

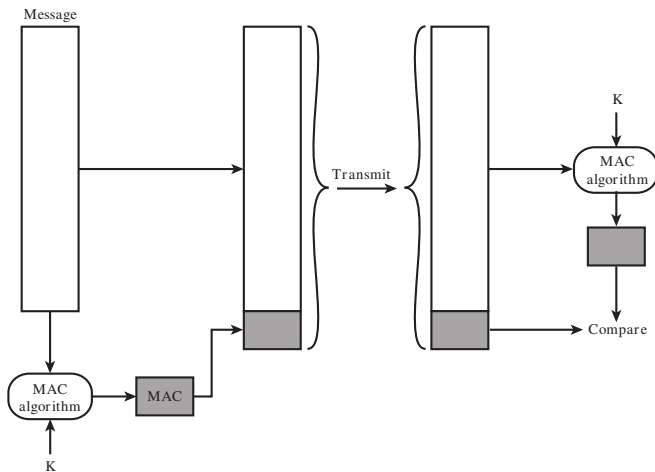
Message Authentication Code (MAC)

- 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

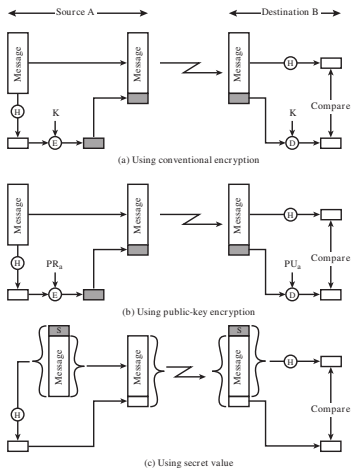
- 1 Asymmetrisk kryptografi
 - Introduktion
 - Kryptosystem
 - Digitala signaturer
- 2 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 3 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - **Hashfunktionsbaserade MAC**
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Hashfunktionsbaserade MAC



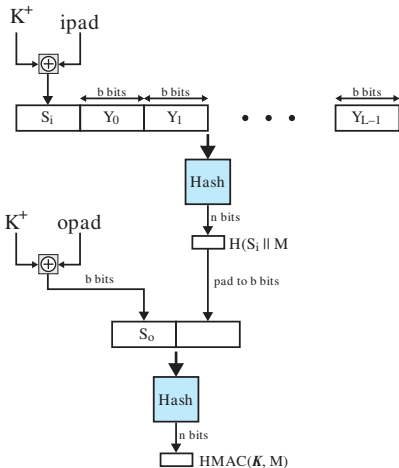
Figur : En översikt av en enkel MAC. Bild: [Sta13].

Hashfunktionsbaserade MAC



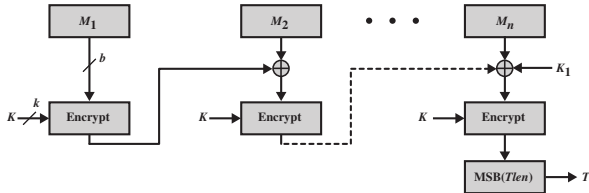
Figur : Exempel på olika former av MAC. Bild: [Sta13].

Hashfunktionsbaserade MAC

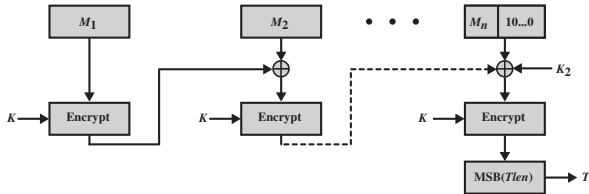


Figur : Hashbaserad MAC kallad HMAC,
 $HMAC(K, M) = h[(K^+ \oplus opad) || h[(K^+ \oplus ipad) || M]]$. Bild: [Sta13].

MAC baserade på blockchiffer



(a) Message length is integer multiple of block size



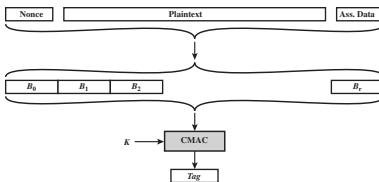
(b) Message length is not integer multiple of block size

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

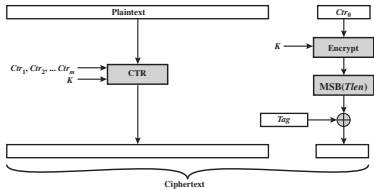
Översikt

- 1 Asymmetrisk kryptografi
 - Introduktion
 - Kryptosystem
 - Digitala signaturer
- 2 Hashfunktioner
 - Introduktion till hashfunktioner
 - Formell behandling av hashfunktioner
- 3 Meddelandeautentisering
 - Message Authentication Code (MAC)
 - Hashfunktionsbaserade MAC
 - MAC baserade på blockchiffer
 - Chiffer med autentisering

Chiffer med autentisering



(a) Authentication



(b) Encryption

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

Referenser I

- [And08] Ross J. Anderson. *Security engineering : a guide to building dependable distributed systems*. Wiley, Indianapolis, IN, 2 utgåvan, 2008.
- [LD05] Stefan Lucks och Magnus Daum. Hash collisions (the poisoned message attack), 2005.
- [Sta11] William Stallings. *Cryptography and network security : principles and practice*. Prentice Hall, Upper Saddle River, 5. ed., international ed. utgåvan, 2011.
- [Sta13] William Stallings. *Network security essentials : applications and standards*. Pearson Education, 5 utgåvan, 2013. International Edition.
- [xkc] xkcd. Security.