Óbudai Egyetem

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

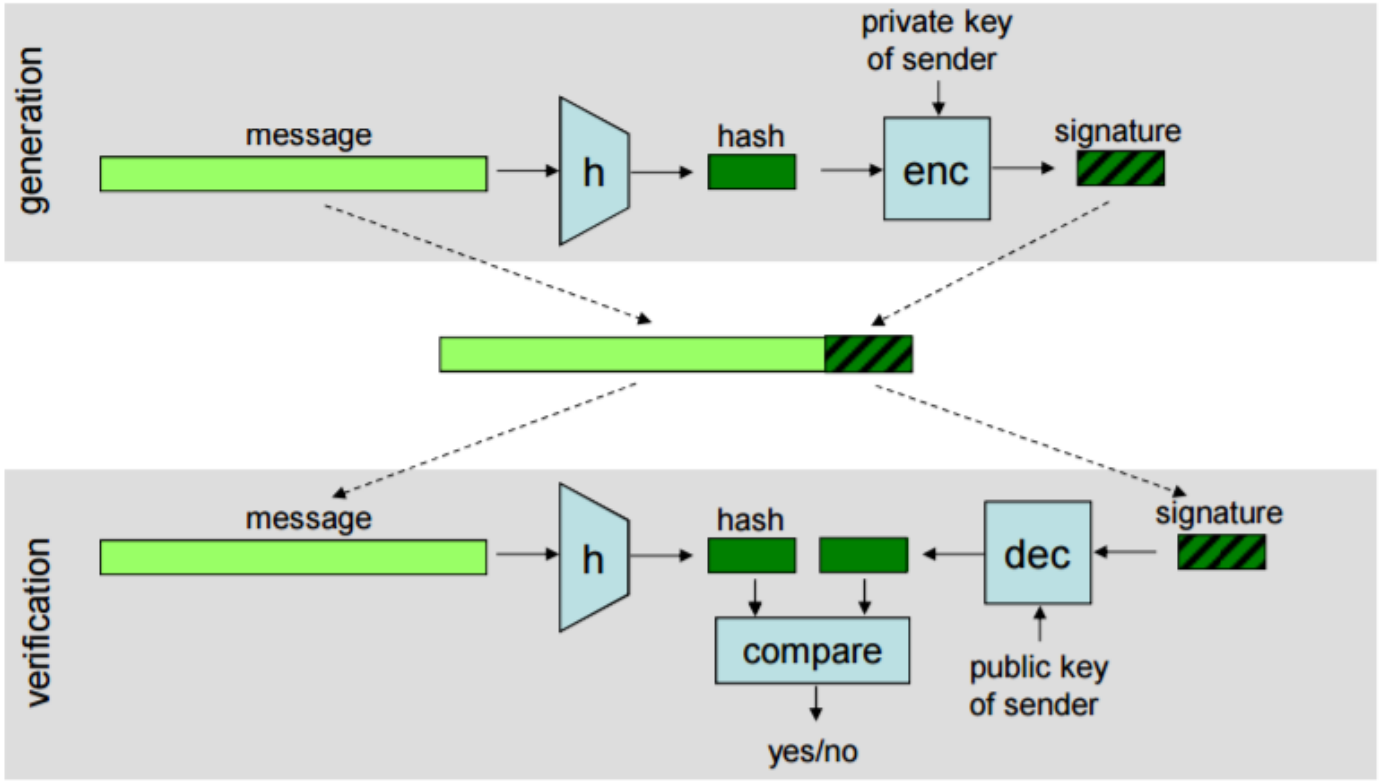
Műszaki területek informatikai biztonsága
Hash függvények

ZENTAI DÁNIEL

ZENTAI.DANIEL@BGK.UNI-OBUDA.HU

Hash függvények

Digitális aláírás:



Hash függvények

H egy hash függvény, ha tetszőleges hosszúságú bitsorozatot fix hosszúságú bitsorozatba képez le, azaz $H:\{0,1\}^* \rightarrow \{0,1\}^n$

Követelmények:

1) Egyirányú: Adott y hash értékhez nehéz olyan x inputot találni, amire $y = H(x)$

2) Gyenge ütközés ellenálló: Adott x inputhoz nehéz olyan $x' \neq x$ inputot találni, amire $H(x') = H(x)$

3) Ütközés ellenálló: Nehéz olyan x és x' input párt találni, amire $x' \neq x$, de $H(x') = H(x)$

Hash függvények

Demo:

md5 hash kiszámítása:
openssl dgst –md5 real.ps
openssl dgst –md5 fake.ps

kulcsgenerálás
openssl genrsa –aes128 –out private.pem 2048
openssl rsa –in private.pem –outform PEM –pubout –out public.pem

aláírás készítése a **real.ps**-re
openssl dgst –md5 –sign private.pem –out real.sgn real.ps

aláírás validálása a **fake.ps**-re
openssl dgst –md5 –verify public.pem –signature real.sgn fake.ps

Hash függvények

Születésnap paradoxon:

Egy 23 fős csoportban nagyjából 50% valószínűséggel van 2 ember, akinek ugyanakkor van a születésnapja.

Általánosabban: Egy n elemű halmazból $\sqrt{n}$ elemet választva visszatevéssel, nagyjából 50% valószínűséggel ismétlődő elem.

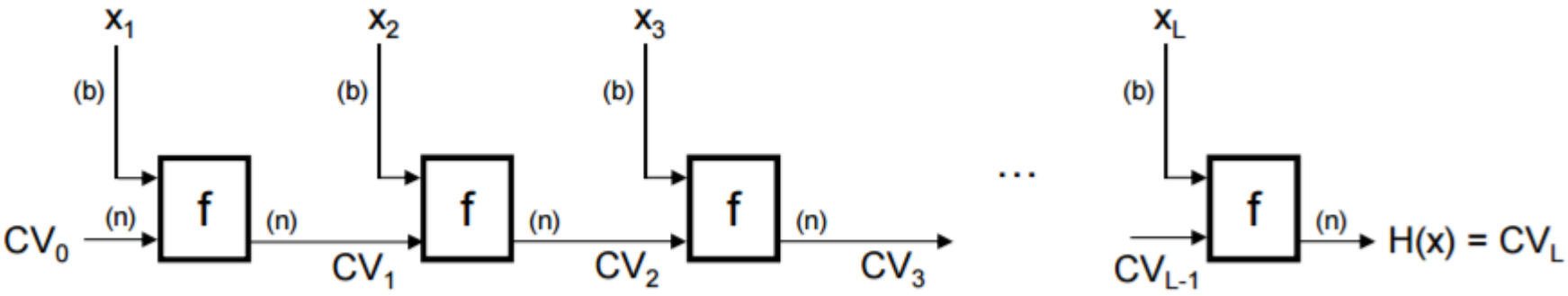
Hash függvényekre vonatkoztatva: Egy n bites hash függvénynek 2^n féle outputja lehet, tehát $\sqrt{(2^n)} = 2^{n/2}$ esetet kipróbálva nagy valószínűséggel lesz ütköző pár.

Következmény: n-et úgy kell választani, hogy még n/2 is nagy legyen.

Hash függvények

Iteratív hash függvények:

Cv_i : chaining variable, CV_0 = IV
x_i : input blokkok
f : kompressziós függvény

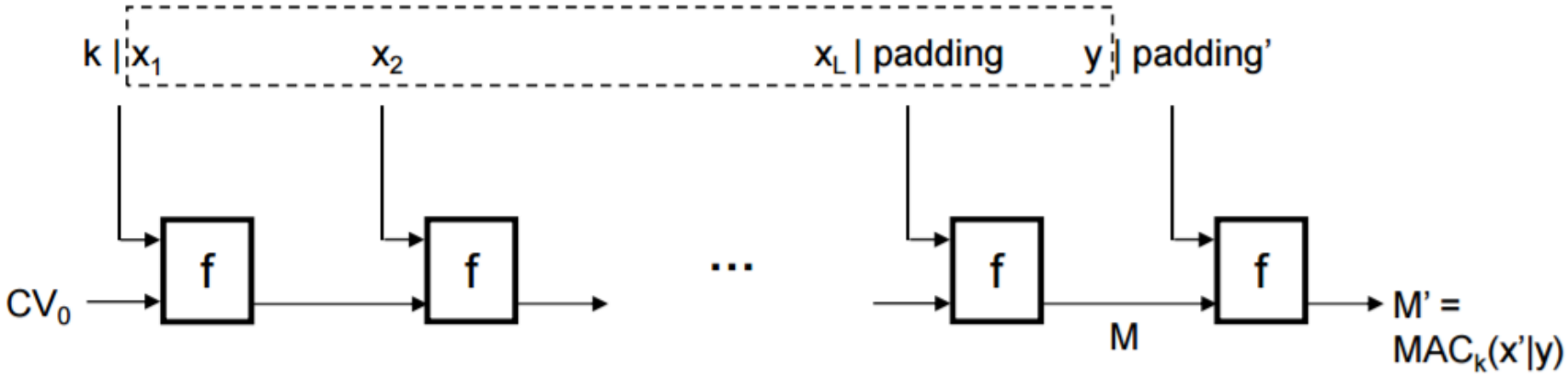


Message Authentication Code (MAC)

A MAC egy kulcsos hash függvény, azaz egy $M : \{0,1\}^* \times \{0,1\}^k \rightarrow \{0,1\}^n$ függvény.

Secret prefix method:
$MAC_K(x) = H(K|x)$

M = H(K|x) ismeretében a támadó ki tudja számolni az x'|y-hoz tartozó MAC-et, ahol x' = x + padding.

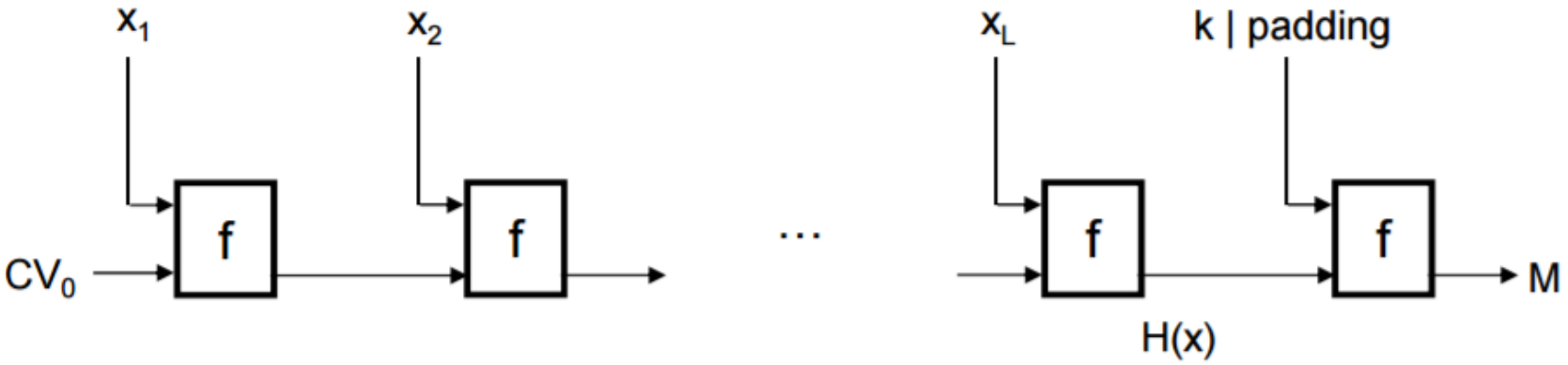


Message Authentication Code (MAC)

Secret suffix method:

$MAC_K(x) = H(x|K)$

Biztonságos, ha H ütközés ellenálló.



HMAC

HMAC: biztonságos, ha H ütközés ellenálló

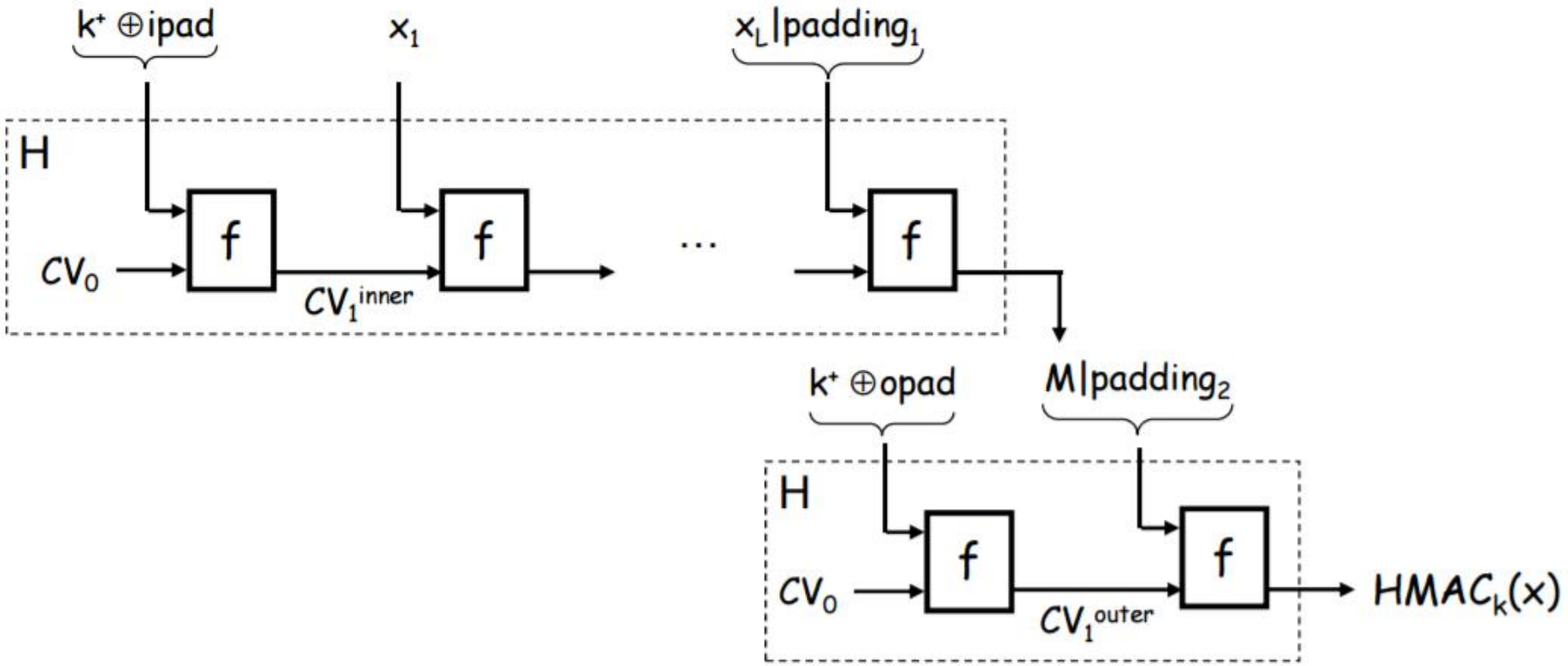
$HMAC_K(x) = H((K^+ \oplus opad) \mid H(K^+ \oplus ipad \mid x))$

K^+=K kiegészítve 0-kal 1 blokk méretűre

ipad=00110110 ismételve 1 blokk hosszan

opad=01011100 ismételve 1 blokk hosszan

HMAC


k⁺ ⊕ipad
x1
xL|padding1
H
f
f
f
CV0
CV1inner
k⁺ ⊕opad
M|padding2
H
f
f
CV0
CV1outer
HMACk(x)

Köszönöm a figyelmet!