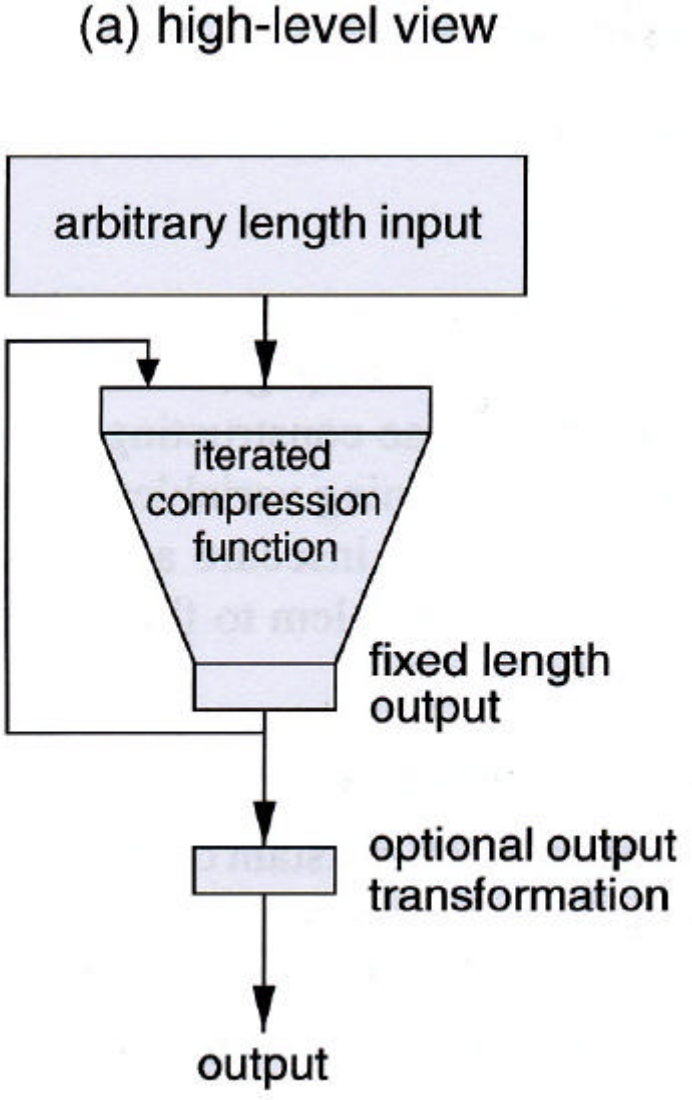
Hash Functions

- Unkeyed Hash
- Birthday paradox
- HMAC
- Keyed Hash

Unkeyed Hash functions

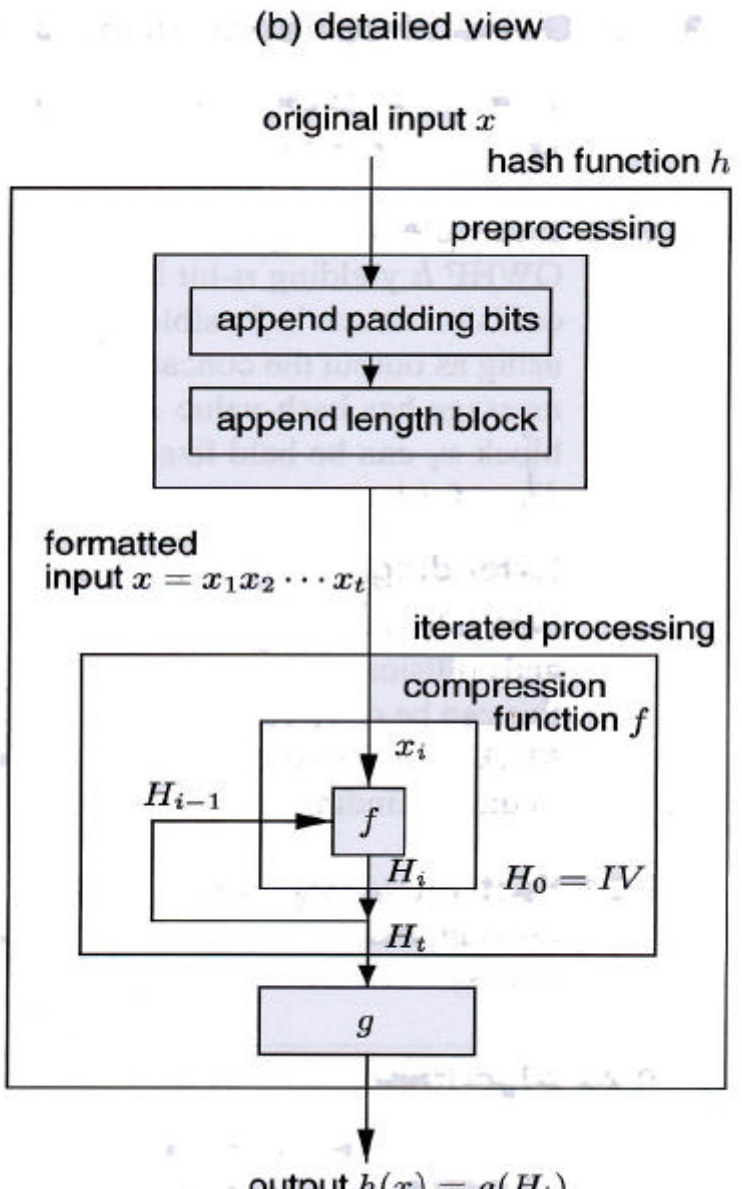


Unkeyed Hash functions

Ho = IV

Hi = f(Hi-1,xi)
1≤i≤t

h(x) = g(Ht)



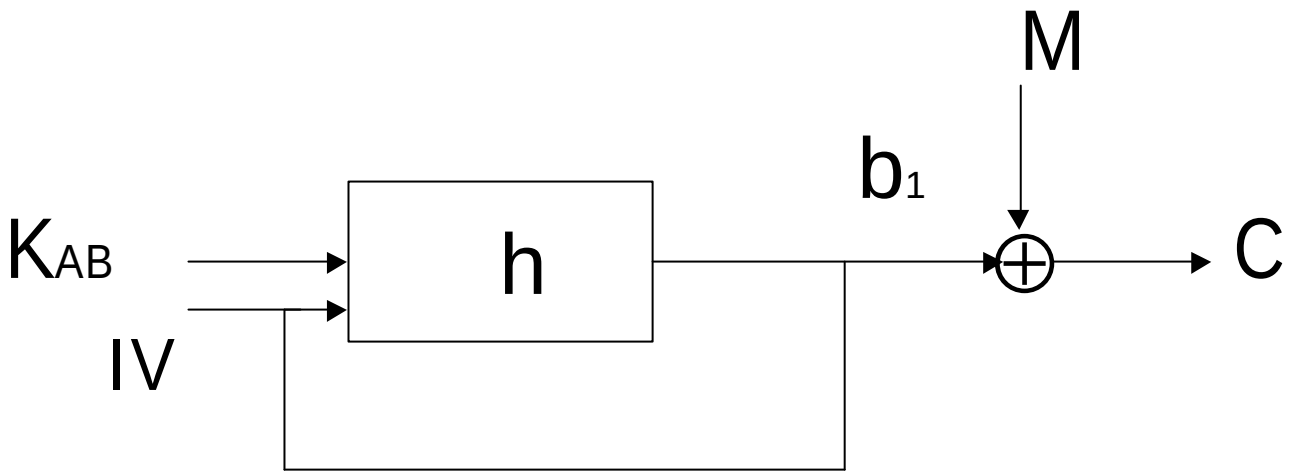
Birthday paradox

- N inputs, K possible outputs
- P>0.5 of guessing if $N>\sqrt{K}$
- Square root lenght of output

Equivalence between Hash and SK

- hash functions for encryption

Similar to DES in OFB mode



$$b_i = h(K_{AB} \mid b_{i-1})$$

Equivalence between Hash and SK

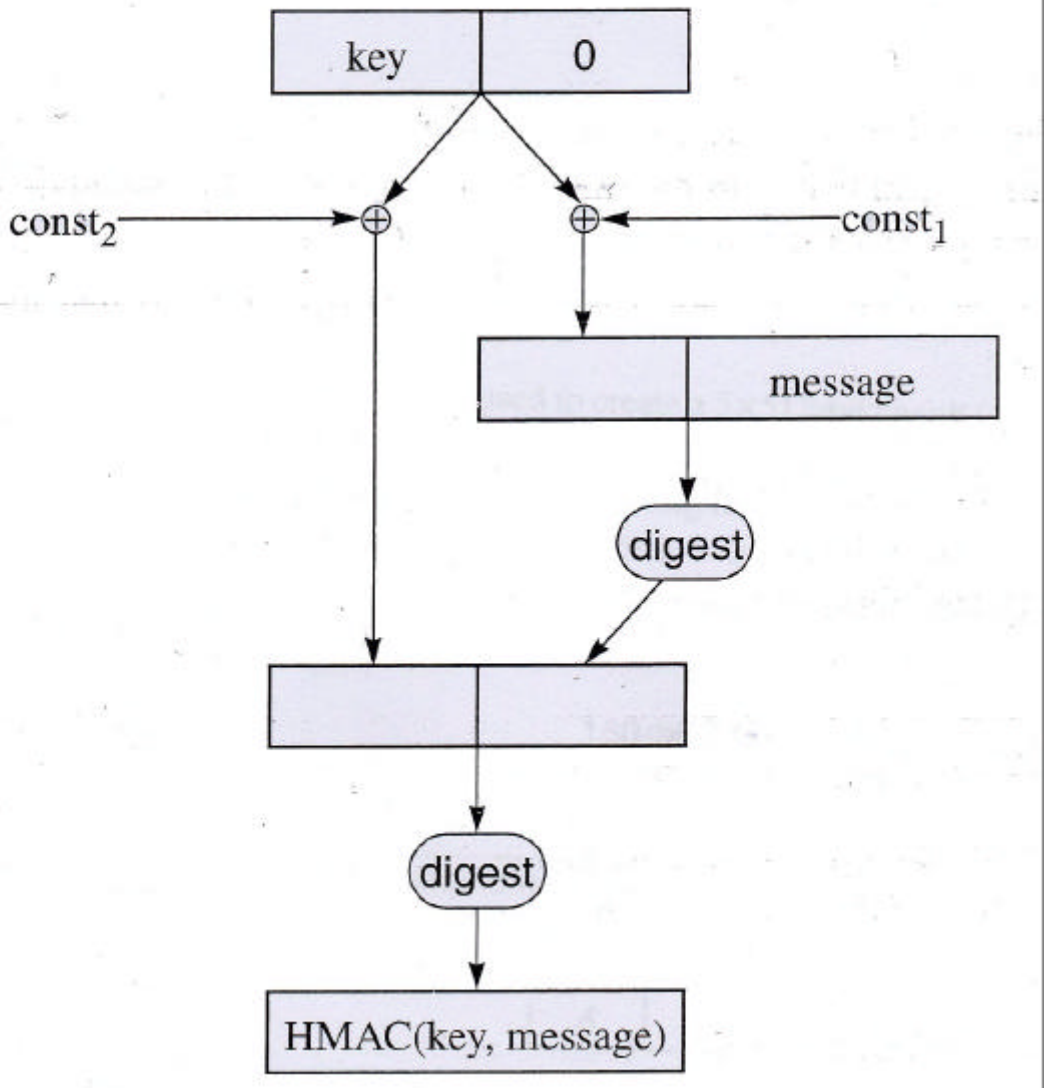
- MAC with hash functions

MAC(x)= h(key|x) MAC'(x|y)=MAC | h(y)

MAC(x)= h(x|key) birthday attack

HMAC

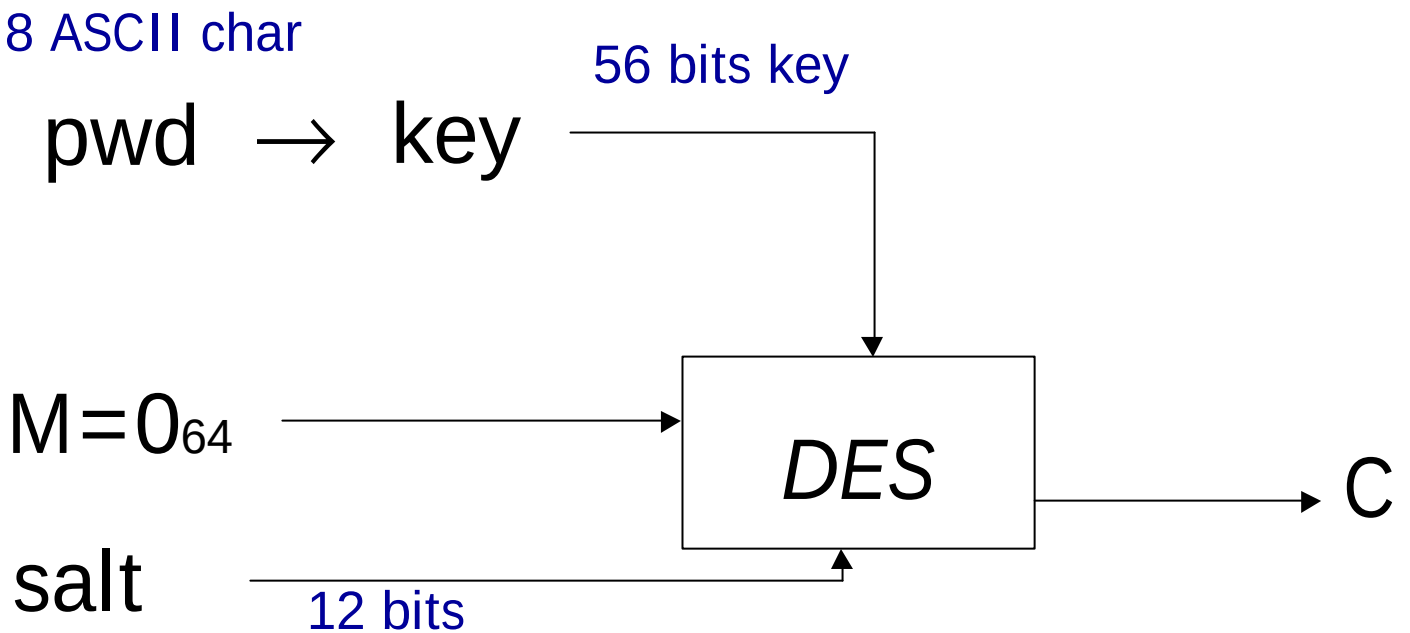
HMAC



Keyed Hash Functions

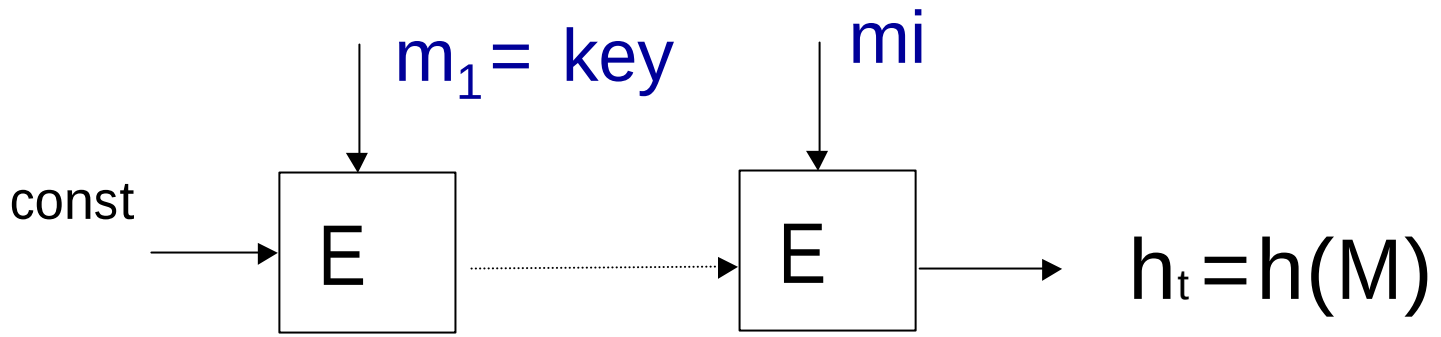
- Use of DES as Hash function
- Es. Unix password

$$hash(salt_A|pwd_A) = DES_{salt}(Key(pwd_A), 0, salt_A)$$



Keyed Hash Functions

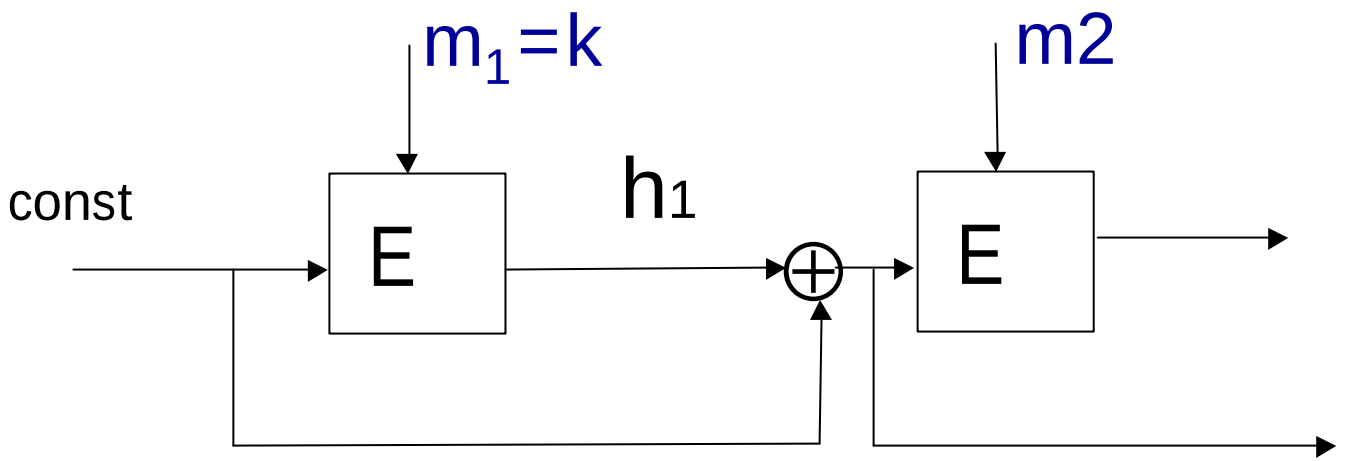
- Use of block cipher to build hash functions



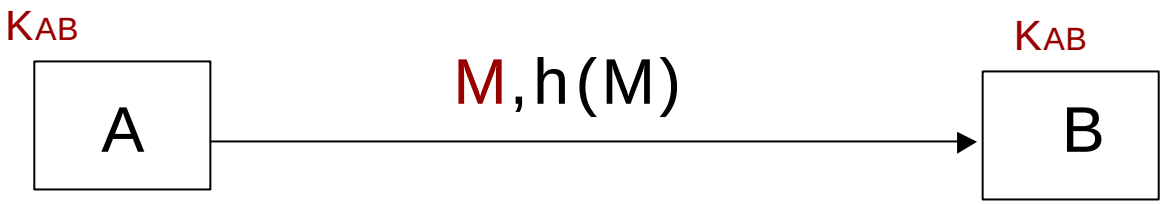
$M = m_1, m_2, .. m_t$

Keyed Hash Functions

- Use of block cipher to build hash functions



Integrity



Unkeyed hash functions

$$h(M) \stackrel{?}{=} h(M)$$

Keyed hash functions

$$HMAC \stackrel{?}{=} E[K_{AB}, M]$$

Asymmetric-Key Cryptography

- Based on a special type of one-way functions: trapdoor functions

- Factorization

- Discrete logarithm

RSA: Rivest Shamir Adleman

p and q large prime $n=pq$

e relatively prime with $\Phi(n)=(p-1)(q-1)$

(n,e) = *public key*

d such that $d=e^{-1} \bmod\{(p-1)(q-1)\}$

(d) =*private key*

$C=M^e(\mathrm{mod}n)$ $M=C^d(\mathrm{mod}n)$

RSA algorithm

$c_i = m_i^e \bmod n$

$m_i = c_i^d \bmod n$

Es. p=47, q=71 n=pq=3337

e no factor in common with (46*70)=3220

Random choose e=79

$d=79^{-1} \bmod 3220 = 1019$

msg=688232687966668 3

$m_1=688$, $m_2=232$, $m_3=687$, $m_4=966$, $m_5=668$, $m_6=003$

$C_1=688^{79} \bmod 3337 = 1570.....$

C= 1570 2756 2091 2276 2423 158

$M_1 = 1570^{1019} \bmod 3337 = 688.....$

Miller-Rabin primality test

Prime number distribution 1/ln N
Given $x \rightarrow \pi(x)=x/\ln x$

Trivial test to see if *N* is prime
(N / all numbers £ ÖN) is even?

Miller-Rabin probabilistic test

Possible attacks

- No provable security
- Problem with some public exponents ($e=3$) with certain conditions (e.g. when $|M| \leq$ cube root N)
- Possible solution: formatting

Discrete Logarithm

- Primitive root *p* is a generator of group *mod p*

$5^1 = 5 \bmod 7$

$5^2 = 25 = 4 \bmod 7$

$5^3 = 125 = 6 \bmod 7$

$5^4 = 2 \bmod 7$

$5^5 = 3 \bmod 7$

$5^6 = 1 \bmod 7$

$y = 5^x$

x discrete log y

mod7 to the base 5

Diffie-Hellman

Chosen and public p and g

Alice		Bob
random Sa		random Sb
$Ta=g^{Sa} \bmod p$		Tb
	$Ta \rightarrow$	
	$\leftarrow Tb$	
$Tb^{Sa} \bmod p$	=	$Ta^{Sb} \bmod p$

Sx private key

Tx public key

W. Diffie, Hellman E.M., "*New directions in cryptography*", IEEE. Trans. Inform. Theory, IT-22, No. 6, pp 644-654. (nov 1976)