3. Funkcije za izračunavanje sažetka poruke

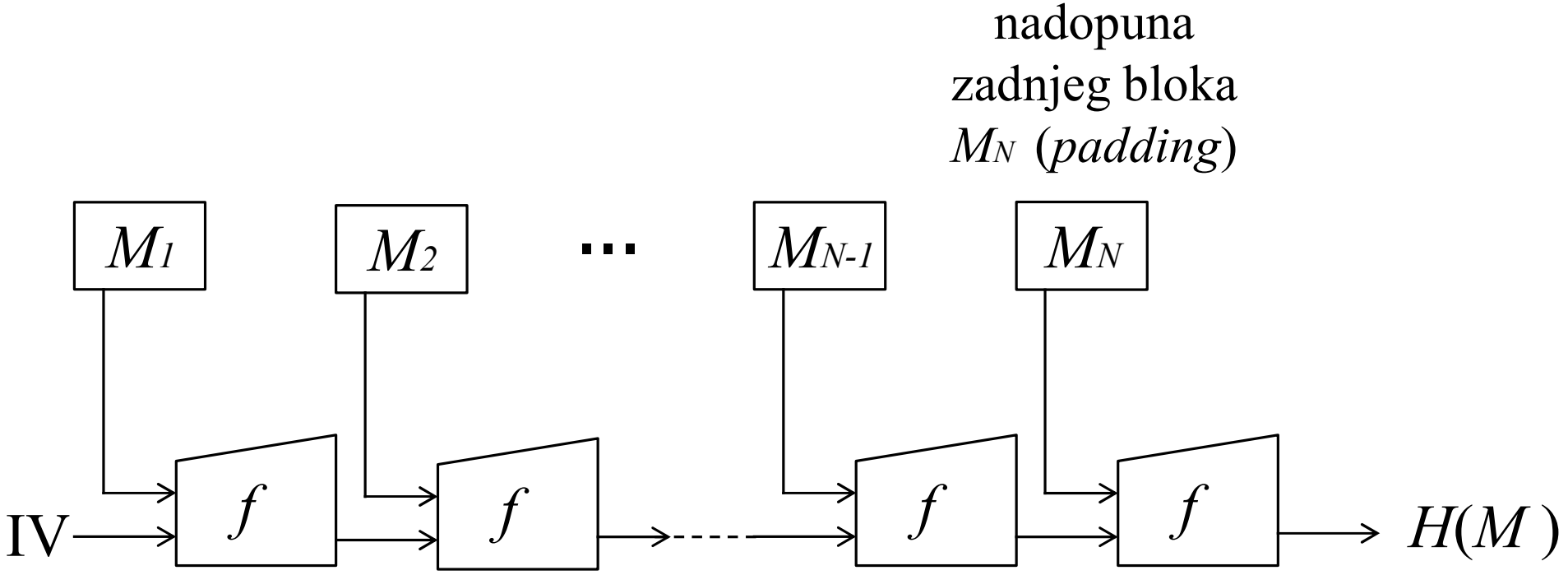
Funkcije sažimanja ili *hash* funkcije

Važna svojstva funkcija za izračunavanje sažetka poruke

- Otpornost na izračunavanje originala
  ili prva domenska otpornost (*preimage resistance*)
  - $H=h(M) \Rightarrow M=h^{-1}(H)$ – inverz ne postoji
  - za dani sažetak H teško je naći poruku M tako da je $H=h(M)$
- Otpornost na izračunavanje poruke koja daje isti sažetak
  ili druga domenska otpornost (*2-nd preimage resistance*)
  - za poznati *M* i $H=h(M)$ je vrlo teško pronaći *M'* koji daje isti *H*
- Otpornost na kolizije (*collision resistance*)
  - nemoguće je pronaći bilo koje dvije poruke *M1* i *M2* za koje se dobiva isti sažetak $h(M1)=h(M2)$
- Difuzija
  - svaka, pa i najmanja promjena ulaznog podatka rezultira velikom i naizgled slučajnom promjenom na izlazu

Konstrukcija *Merkle–Damgård*

- koriste je MD5, SHA-1, SHA-2 i druge funkcije za izračunavanje sažetka poruke



MD5

- *Message Digest* = sažetak poruke
- proizvodi 128-bitovni sažetak
- izvorni tekst dijeli se na blokove duljine **512** bitova
- zadnji blok teksta se nadopunjuje (engl. *padding*) do 512 bitova tako da se:

  - iza zadnjeg bita teksta dodaje jedna jedinica

  - nakon 1 upisuju se nule tako da u bloku preostanu 64 bita

  - u ta 64 bita se upisuje bitovna duljina izvorne poruke
- svaki blok se dijeli na 16 podblokova po 32 bita :

$$M_0 , M_1 , M_2, \ldots, M_{15}$$

Funkcije i konstante algoritma MD5

- sažetak H od 128 bitova sastoji se od 4 nadovezanih 32-bitovnih varijabli koje se inicijaliziraju s vrijednostima:

$$A_0 = 01234567_{16} \quad B_0 = 89ABCDEF_{16}$$
$$C_0 = FEDCBA98_{16} \quad D_0 = 76543210_{16}$$

- postupak se obavlja u 64 koraka podijeljena u 4 kruga

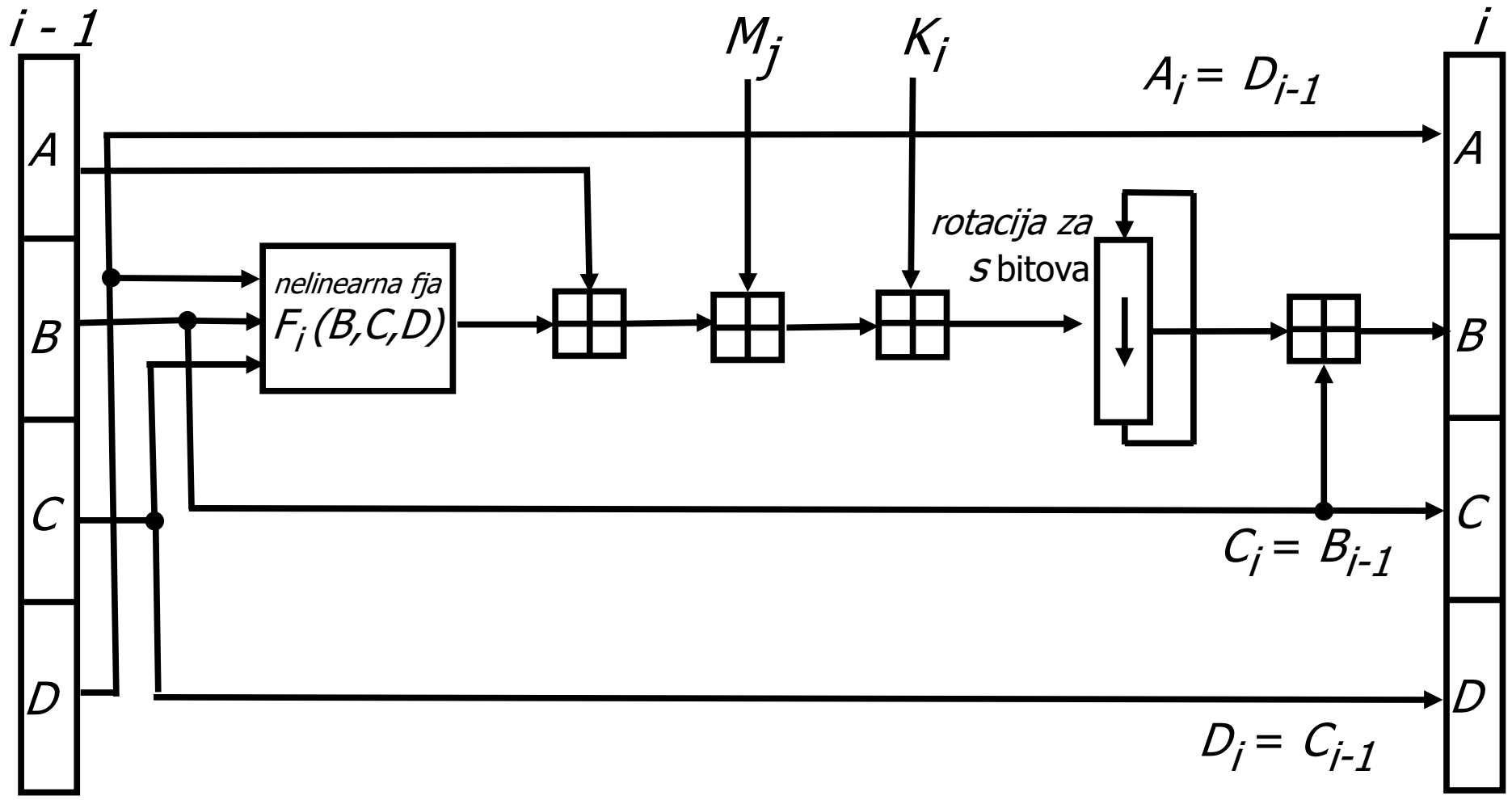
  $\Rightarrow$ svaki krug se sastoji od 16 koraka

- u svakom krugu koristi se jedna od četiri funkcije

$$\mathbf{F_i(x,y,z) = (X \wedge Y) \vee (!X \wedge Z),} \qquad 1 \le i \le 16$$
$$\mathbf{F_i(x,y,z) = (X \wedge Y) \vee (X \wedge !Z),} \qquad 17 \le i \le 32$$
$$\mathbf{F_i(x,y,z) = X \oplus Y \oplus Z,} \qquad 33 \le i \le 48$$
$$\mathbf{F_i(x,y,z) = y \oplus (X \wedge !Z),} \qquad 49 \le i \le 64$$

- u svakom koraku koristi se sljedeća varijabla:

$$\boldsymbol{K_i = 2^{32} \times abs(sin(i)),} \qquad 1 \le i \le 64$$



$$B_i = B_{i-1} + ((A_{i-1} + F_i(B_{i-1}, C_{i-1}, D_{i-1}) + M_j + K_i) <<< s)$$

$S = A\,B\,C\,D$, gdje su $A = A_{64} + A_0 \quad B = B_{64} + B_0$

$C = C_{64} + C_0 \quad D = D_{64} + D_0$

SHA-1

- proizvodi **160**-bitovni sažetak
- podjela jasnog teksta na blokove od 512 bitova i nadopuna zadnjeg bloka (*padding*) odvija se na jednak način kao i kod algoritma MD5
- sažetak *H* od 160 bitova sastoji se od 5 nadovezanih 32-bitovnih varijabli koje se inicijaliziraju s vrijednostima:

$A_0 = 67452301_{16}$ $B_0 = EFCDAB89_{16}$

$C_0 = 98BADCFE_{16}$ $D_0 = 10325476_{16}$ $E_0 = C3D2E1F0_{16}$

Funkcije i konstante algoritma SHA-1

- podblokovi M_0 , …, M_{15} služe za stvaranje 80 riječi

$$W_i = M_{i-1}, \qquad 1 \le i \le 16$$

$$W_i = (W_{i-3} \oplus W_{i-8} \oplus W_{i-14} \oplus W_{i-16}) \lll 1, \qquad 17 \le i \le 80$$

- sažimanje svakog podbloka obavlja se u 4 kruga, svaki s 20 koraka, tj. ukupno 80 koraka, a u svakom krugu koristi se jedna od četiri funkcije i konstante:

$$F_i = (X \wedge Y) \vee (\neg X \wedge Z), \qquad 1 \le i \le 20$$

$$F_i = X \oplus Y \oplus Z, \qquad 21 \le i \le 40$$

$$F_i = (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z), \qquad 41 \le i \le 60$$

$$F_i = X \oplus Y \oplus Z, \qquad 61 \le i \le 80$$

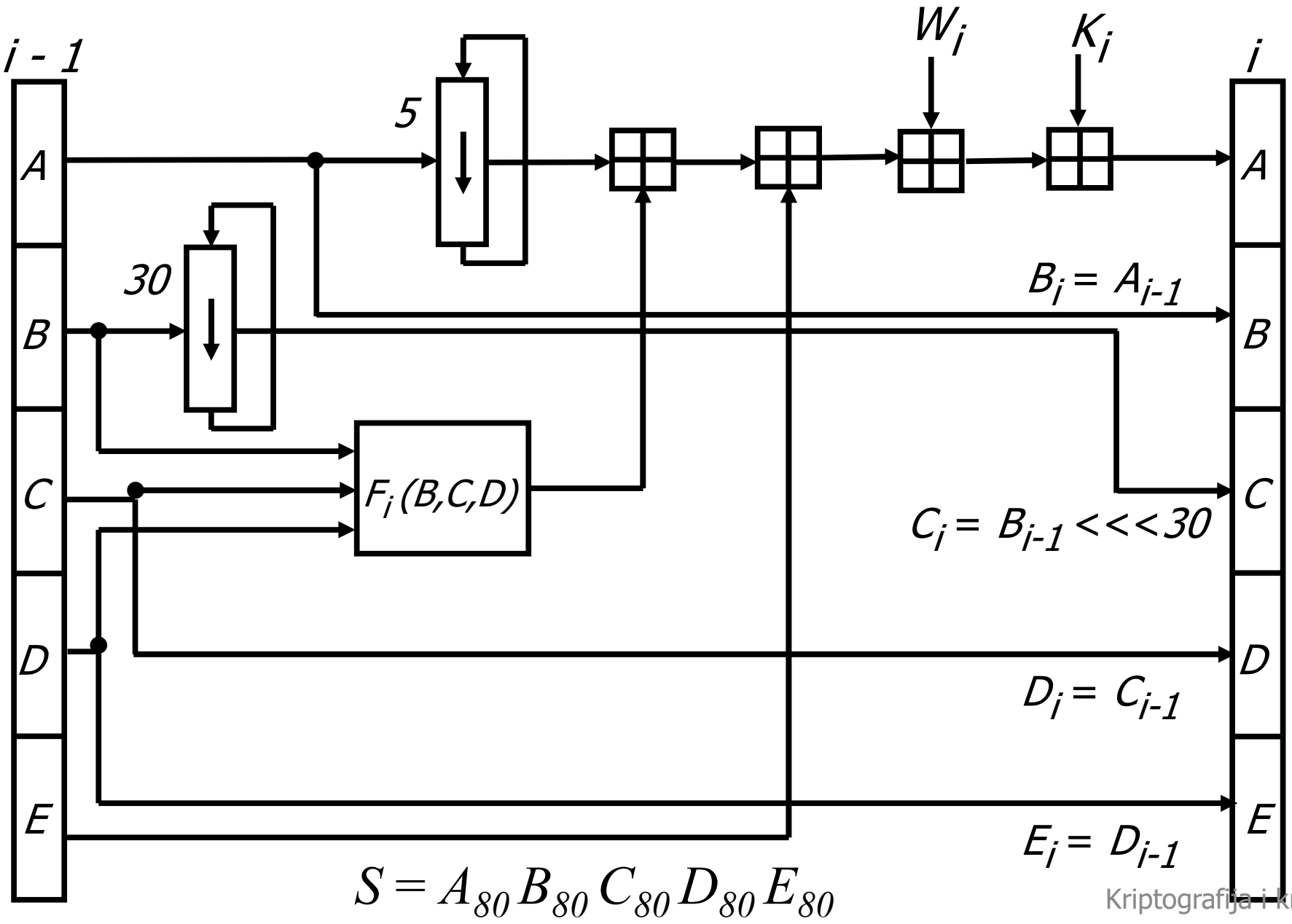
$$K_i = 5A827999_{16}, \qquad 1 \le i \le 20$$

$$K_i = 6ED9EBA1_{16}, \qquad 21 \le i \le 40$$

$$K_i = 8F1BBCDC_{16}, \qquad 41 \le i \le 60$$

$$K_i = CA62C1D6_{16}, \qquad 61 \le i \le 80$$

$A_i = (A_{i-1} <<< 5) + F_i(B_{i-1}, C_{i-1}, D_{i-1}) + E_{i-1} + W_i + K_i$



$$S = A_{80}\, B_{80}\, C_{80}\, D_{80}\, E_{80}$$

SHA-2

- osmislila NSA
- NIST publicirao 2001 u vrijeme natječaja za SHA-3
- skup funkcija:
  - SHA-224 (veličina bloka na ulazu je 512 bita = 64 bajta)
  - SHA-256 (veličina bloka na ulazu je 512 bita = 64 bajta)
  - SHA-384 (veličina bloka na ulazu je 1024 bita = 128 bajtova)
  - SHA-512 (veličina bloka na ulazu je 1024 bita = 128 bajtova)

Algoritam	Sažetak	Stanje	Blok	Poruka	Arhitektura	Broj rundi	Funkcije
SHA-1	**160**	**160**	**512**	**$2^{64} - 1$**	**32**	**80**	**+, and, or, xor, rot**
SHA-256/224	**256/224**	**256**	**512**	**$2^{64} - 1$**	**32**	**64**	**+, and, or, xor, shift, rot**
SHA-512/384	**512/384**	**512**	**1024**	**$2^{128} - 1$**	**64**	**80**	**+, and, or, xor, shift, rot**

SHA-2

- http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
- zadnji blok teksta se nadopunjuje do 512 bitova na isti način kao i SHA-1
- poruka se podijeli na blokove od po 512 bita:

$$M^{(1)}, M^{(2)}, \ldots, M^{(N)}$$

- svaki blok se dijeli na 16 podblokova po 32 bita :

$$M_0 , M_1 , M_2, \ldots, M_{15}$$

- $H^{(0)} = a_0 b_0 c_0 d_0 e_0 f_0 g_0 h_0$

a_0=6a09e667 e_0=510e527f
b_0=bb67ae85 f_0=9b05688c
c_0=3c6ef372 g_0=1f83d9ab
d_0=a54ff53a h_0=5be0cd19

Funkcije i konstante algoritma SHA-2

$$Ch(X,Y,Z) = (X \wedge Y) \oplus (\neg X \wedge Z)$$

$$Maj(X,Y,Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$$

$$S_0(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$$

$$S_1(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{22}(x)$$

$$F_0(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x)$$

$$F_1(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$$

$$K_t = 5a827999, \quad za\ 0 \leq t \leq 15$$

$$K_t = 6ed9eba1, \quad za\ 16 \leq t \leq 31$$

$$K_t = 8f1bbcdc, \quad za\ 32 \leq t \leq 47$$

$$K_t = ca62c1d6, \quad za\ 48 \leq t \leq 64$$

- koristi se zbrajanje po modulu 2^{32}

SHA-2

za i=1 do N , tj. za svaki od N blokova računaj

Priprema (izračunavanje Wt)

$W_t = M_t^{(i)}$, $0 \leq t \leq 15$

$W_t = F_1(W_{t-2}) + W_{t-7} + F_0(W_{t-15}) + W_{t-16})$, $16 \leq t \leq 63$

Postavljanje početnih vrijednosti iz prošlog kruga ili postavljanje konstanti ako se radi o prvom krugu

$a=H_0^{(i-1)}$ $b=H_1^{(i-1)}$ $c=H_2^{(i-1)}$ ... $h=H_7^{(i-1)}$

za t=0 do 63 radi // u 64 koraka

Računaj a,b,c,d,e,f,g,h

$H_0^{(i)}=a+H_0^{(i-1)}$

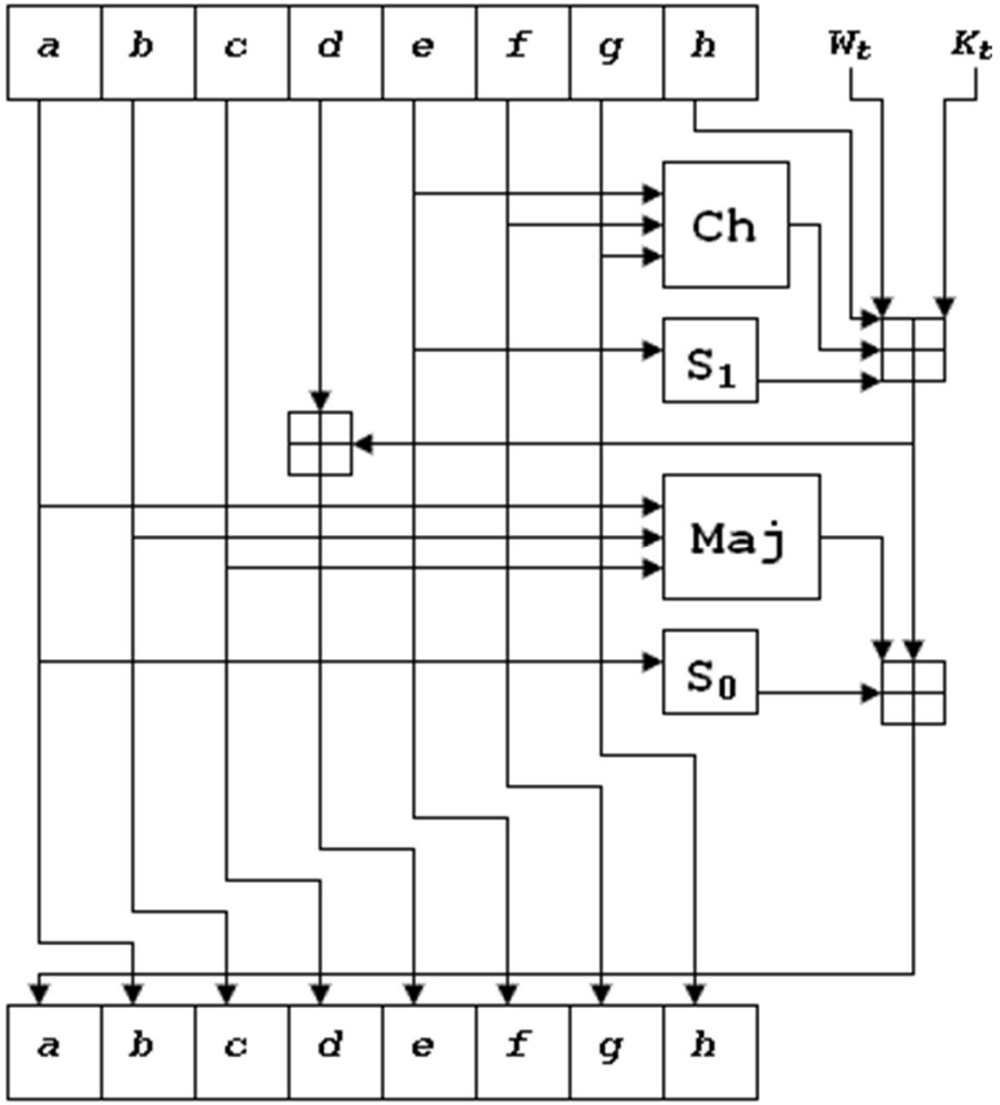
$H_1^{(i)}=b+H_1^{(i-1)}$

...

$H_7^{(i)}=h+H_7^{(i-1)}$

SHA-2

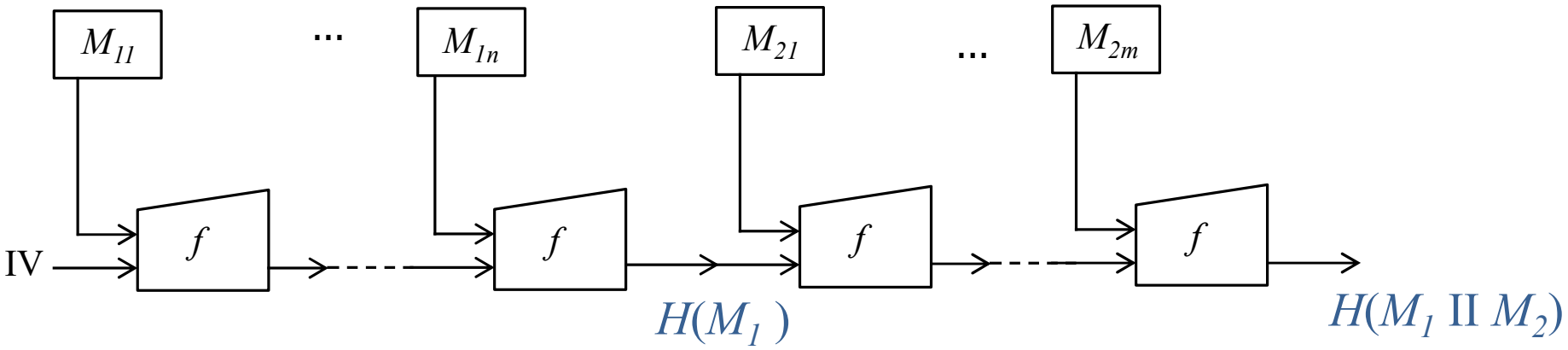
Računaj a,b,c,d,e,f,g,h:



Napad na tajni sufiks poruke

(*engl. Length Extension Attack* odnosno *Attack Against Secret Suffix*)

- algoritmi zasnovani na konstrukciji Merkle–Damgård su osjetljivi na tu vrstu napada
- napadač na temelju poznatog sažetka $H(M_1)$ i duljine poruke M_1, a bez da poznaje poruku M_1, može umetnuti dodatne podatke na kraj poruke M_1, tj. može dodati proizvoljnu dodatnu poruku M_2 i izračunati $H(M_1 \text{ II } M_2)$



SHA-3

- 2.11.2007. – NIST raspisuje natječaj za SHA-3
- informacije o natječaju su dostupne na http://csrc.nist.gov/groups/ST/hash/sha-3/index.html
- konačni izbor 2.10.2012. godine
- do 31.10.2008. zabilježeno je 64 prijava:

Abacus	ARIRANG	AURORA	BLAKE	Blender	BMW	BOOLE	Cheetah
CHI	CRUNCH	CubeHash	DCH	Dynamic SHA	Dynamic SHA2	ECHO	ECOH
ENDO-R	EnRUPT	ESSENCE	FSB	Fugue	Groestl	Hamsi	HASH 2x
JH	Keccak	Khichidi-1	LANE	Lesamnta	Luffa	LUX	Maraca
MCSSHA-3	MD6	MeshHash	NaSHA	NKS 2D	Ponic	SANDstorm	Sarmal
Sgail	Shabal	SHAMATA	SHAvite-3	SIMD	Skein	Spectral Hash	StreamHash
SwiFFTX	Tangle	TIB3	Twister	Vortex	Wamm	Waterfall	ZK-Crypt
?	?	?	?	?	?	?	?

SHA-3

- 24.6.2009. objavljena je lista od 14 kandidata za drugi krug:
  - BLAKE
  - BMW - Blue Midnight Wish
  - CubeHash (Bernstein)
  - ECHO (France Telecom)
  - Fugue (IBM)
  - Groestl (Knudsen)
  - Hamsi
  - JH
  - Keccak (Daemen)
  - Luffa
  - Shabal
  - SHAvite-3
  - SIMD
  - Skein (Schneier)

	ARIRANG		BLAKE		BMW		Cheetah
CHI	CRUNCH	CubeHash			Dynamic SHA2	ECHO	
		ESSENCE	FSB	Fugue	Groestl	Hamsi	
JH	Keccak		LANE	Lesamnta	Luffa		
	MD6					SANDstorm	
	Shabal		SHAvite-3	SIMD	Skein		
SwiFFTX							

SHA-3

- 9.12.2010. objavljen je popis 5 finalista
- 2.10.2012. proglašen pobjednik

- BLAKE
- Groestl (Knudsen)
- JH
- Keccak (Daemen)
- Skein (Schneier)

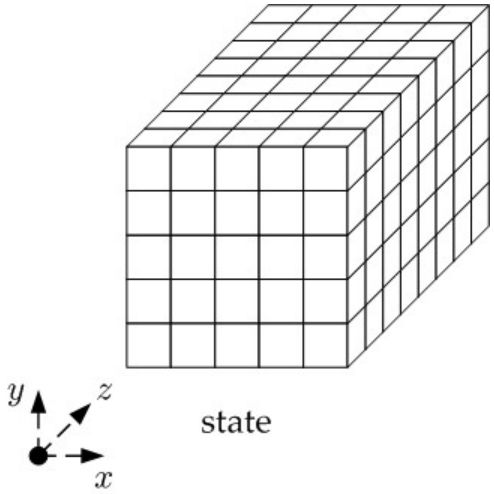
			BLAKE		BMW		
		CubeHash				ECHO	
				Fugue	Groestl	Hamsi	
JH	Keccak				Luffa		
	Shabal		SHAvite-3	SIMD	Skein		

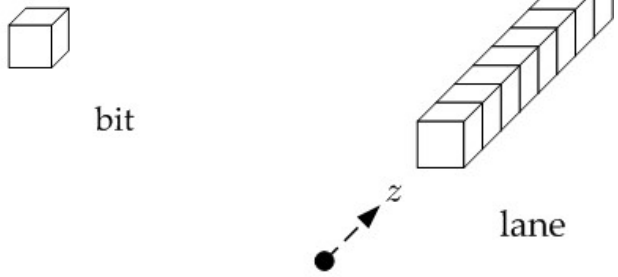
SHA-3

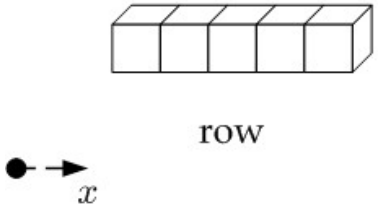
- autori su Guido Bertoni, Joan Daemen (autor AES-a), Michaël Peeters, and Gilles Van Assche
- značajno brži od ostalih finalista
- sažeci su jednake duljine kao i kod SHA-2, ali se veličine ulaznih blokova razlikuju:
  - SHA3-224 (veličina ulaznog bloka 1152 bitova)
  - SHA3-256 (veličina ulaznog bloka 1088 bitova)
  - SHA3-384 (veličina ulaznog bloka 832 bitova)
  - SHA3-512 (veličina ulaznog bloka 576 bitova)
- nadopunjavanje zadnjeg bloka teksta (*padding*) je izmijenjeno i obavlja se prema shemi M || 10*1
  - SHA-2: M II 10* II 64-bita za duljinu poruke
  - izvorni prijedlog autora algoritma Keccak: M II 10*1000000

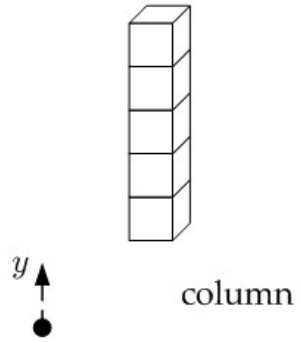
SHA-3: stanje, bit, traka, redak i stupac

- $X = Y = 5$
- duljina trake $Z = w \in \{1, 2, 4, 8, 16, 32, 64\}$
- w je duljina CPU riječi
- Keccak-$f[b]$ gdje je b broj bitova stanja $b = 25w$
  b $\in \{25, 50, 100, 200, 400, 800, 1600\}$
- slike su preuzete sa http://keccak.noekeon.org/

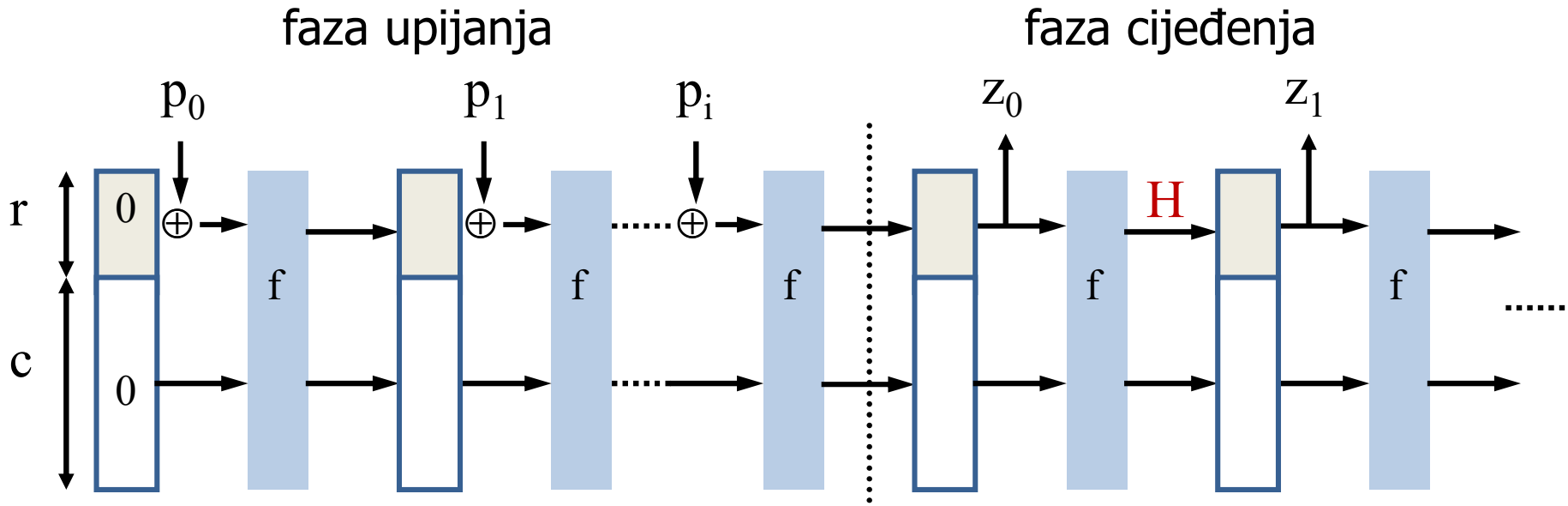








Spužvasta konstrukcija algoritma SHA-3



- **25w = c + r** = 1600 za 64-bitne riječi ili 800 za 32-bitne riječi, itd.
- kapacitet c = 2 x veličina sažetka i **veličina bloka** (ostatak) r = 25w - c
  - SHA3-224: c = 448, r = 800 – 448 = 352 bitova = 44 bajta
  - SHA3-256: c = 512, r = 800 – 512 = 288 bitova = 36 bajta
  - SHA3-384: c = 768, r = 832 bitova = 104 bajta
  - SHA3-512: c = 1024, r = 576 bitova = 72 bajta

SHA-3: funkcija *f*

- obavlja se u n_r koraka: $n_r = 12+2l$, gdje je $2^l = w$
- za $w = 64 = 2^6$, $n_r = 24$ koraka

```
Keccak-f[b](A)
    za i 0 do nr-1
        A = Round[b](A, RC[i])
    return A
```

- funkcija *f* se sastoji od poziva pet osnovnih funkcija koje manipuliraju s bitovima *stanja* :
  - **θ** (*theta*)
  - **ρ** (*rho*)
  - **π** (*pi*)
  - **χ** (*chi*)
  - **ι** (*iota*)

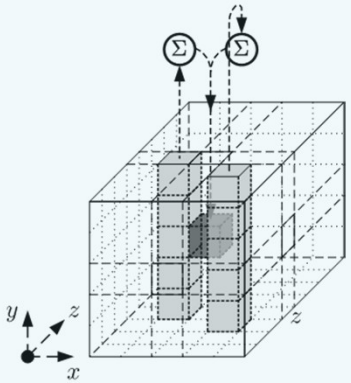
SHA-3: funkcija *f*

```
Keccak-f[b](A){
      za i 0 do nr-1
         // (x,y)∈(0…4,0…4)
         // funkcija θ
         C[x] = A[x,0] xor A[x,1] xor A[x,2] xor
                A[x,3] xor A[x,4];
         D[x] = C[x-1] xor rot(C[x+1],1);
         A[x,y] = A[x,y] xor D[x];

         // funkcije ρ i π
         B[y,2*x+3*y] = rot(A[x,y], r[x,y]);

         // funkcija χ
         A[x,y] = B[x,y] xor ((not B[x+1,y]) and
                    B[x+2,y]);

         // funkcija ι
         A[0,0] = A[0,0] xor RC
      return A;
```

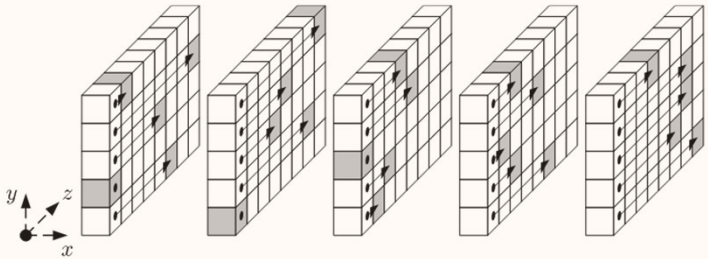
Funkcije θ (*theta*), ρ (*rho*), π (*pi*), χ (*chi*) i ι (iota)

- manipuliraju bitovima stanja

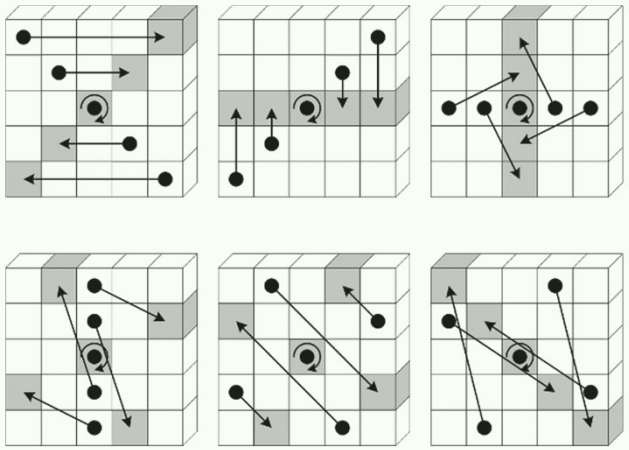
funkcija *theta*

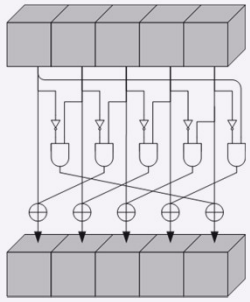


funkcija *rho*



funkcija *pi*





funkcija *chi*

```
a[i][j][k] ⊕=
¬a[i][j+1][k]
& a[i][j+2][k]
```

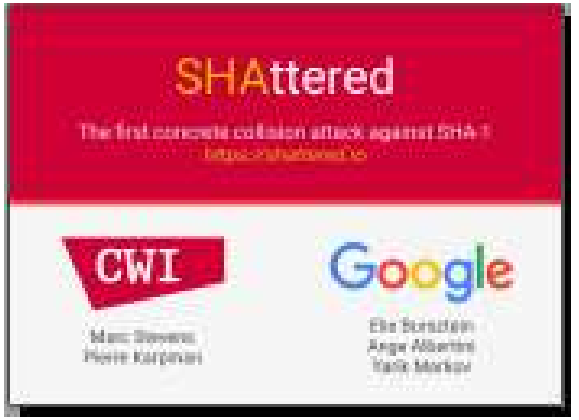
funkcija *iota*

```
A[0,0] ⊕= RC[i]
RC[i] - konstante
```

Napadi na funkciju sažimanja SHA

- 1993. – objavljen SHA-0
- 1995. – NSA je predložila SHA-1 kao zamjenu za SHA-0
- 1998. – objavljen uspješan napad na SHA-0, ali ne i na SHA-1
- 2001. – NSA predlaže SHA-2
- 2005. – uspješan napad na SHA-1
- 2007. – NIST raspisuje natječaj za SHA-3 i preporuča SHA-2
- 2012. – proglašen pobjednik natječaja SHA-3: Keccak
- 2017. – uspješan napad na SHA-1:
  - dva različita PDF dokumenta daju isti sažetak (Marc Sevens ispred svih u suradnji s tvrtkom Google)
  - https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

- za pronalazak kolizije potrebno je:
  - MD5 → 1 pametni telefon i 30 s
  - SHA-1 → grubom silom i 12 000 000 GPU godina
  - SHA-1 → algoritam Shattered i 110 GPU godina



Primjer napada na *hash* funkcije
Rođendanski napad

- engl. *birthday attack*
- vjerojatnost da dvije osobe u dvorani u kojoj je ukupno $k=1.2 \cdot 365^{1/2} = 23$ ljudi imaju isti dan rođendan je veća od 50%
- analogno:
  vjerojatnost da dvije poruke iz skupa od $k=1.2\ (2^n)^{1/2} = 1.2 \cdot 2^{n/2}$ poruka daju isti sažetak je veća od 50%, gdje je n duljina sažetka u bitovima

Primjer napada

```
M1.txt
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 87 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 71 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd f2 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a c7 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 cc 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a d8 35 cc a7 e3
M2.txt
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 07 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 f1 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd 72 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a 47 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 4c 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a 58 35 cc a7 e3

MD5 Sum(M1.txt) = a4c0d35c95a63a805915367dcfe6b751
MD5 Sum(M2.txt) = a4c0d35c95a63a805915367dcfe6b751
```

Primjer napada

```
M1.txt
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 87 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 71 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd f2 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a c7 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 cc 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a d8 35 cc a7 e3
M2.txt
00000000 d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
00000010 2f ca b5 07 12 46 7e ab 40 04 58 3e b8 fb 7f 89
00000020 55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 f1 41 5a
00000030 08 51 25 e8 f7 cd c9 9f d9 1d bd 72 80 37 3c 5b
00000040 96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
00000050 35 73 9a 47 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
00000060 75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 4c 15 5c
00000070 ed 74 cb dd 5f c5 d3 6d b1 9b 0a 58 35 cc a7 e3

MD5 Sum(M1.txt) = a4c0d35c95a63a805915367dcfe6b751
MD5 Sum(M2.txt) = a4c0d35c95a63a805915367dcfe6b751
```

Digitalni certifikat

FER-ov digitalni certifikat od 2008 do 2018

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 75 (0x4b)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=US, ST=WA, L=Seattle, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=certs@thawte.com
       Validity
           Not Before: May 13 23:33:08 2008 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=HR, ST=Grad Zagreb, L=Zagreb, O=FER, OU=CIP,
                CN=webmail.fer.hr/emailAddress=korisnik@webmail.fer.hr
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (2048 bit):
                    00:cd:66:28:fb:b8:b3:b7:e0:72:77:48:2d:08:04:
                    e1:6d:1c:c5:4f:57:73:0c:e6:db:3b:8e:cd:c6:25:
                    61:7f:60:c9:da:a3:9f:1d:fa:d8:ef:00:7b:f9:54:
                    65:ab:7e:9e:9b:6d:ff:d4:12:ad:f8:ac:87:6e:83:
                    ec:65:5f:b4:2d:eb:b8:dc:1c:d7:32:b7:46:a5:e3:
                    a1:6c:0b:4c:1b:0c:89:0a:fb:0e:3a:c0:0f:af:b2:
                    62:1d:2f:60:e4:b1:27:b4:7c:59:00:2c:19:e9:f3:
                    a3:88:fe:01:d6:56:be:26:c7:f8:42:b1:79:39:98:
                    a1:b4:4a:84:dd:20:ca:e7:a9:db:6d:a6:73:88:e7:
                    81:8b:3e:81:3d:00:e5:5d:7f:3d:9b:cd:ba:9b:28:
                    88:88:7f:d7:69:2c:66:eb:8f:79:b8:ec:bc:bb:76:
                    67:b1:00:2a:70:bd:f1:21:66:6f:ba:74:81:82:30:
                    02:c0:a8:57:f8:9f:76:02:df:7f:49:44:4a:32:93:
                    48:a4:25:73:47:10:21:20:fe:b6:d2:09:1a:60:4f:
                    a5:d9:df:ea:55:49:43:c6:ce:96:0b:7d:a7:22:c1:
                    3e:5b:28:2e:2c:04:7a:b2:93:89:db:d8:2b:59:86:
                    a3:0a:c1:6f:f9:56:b2:a5:71:4c:4b:74:f3:b8:a1:
                    b4:65
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption
       07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
       a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
       e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
       b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
       70:47
```

Primjer gdje bi se teoretski napad mogao primijeniti

Aktualan FER-ov digitalni certifikat

Pristup web stranicama FER-a:

The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM.

```
Certificate:
    Data: Version: 3 (0x2)
        Serial Number: 0a:2f:ab:75:d4:a1:ee:f5:ea:df:74:15:aa:fd:47:c4
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA SSL CA 3
    Validity  Not Before: May 13 00:00:00 2018 GMT
              Not After : May 20 12:00:00 2020 GMT
    Subject: C=HR, L=Zagreb, O=Sveu\xC4\x8Dili\xC5\xA1te u Zagrebu, OU=CIP,
      CN=*.fer.unizg.hr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c6:bb:ca:00:b5:40:96:b3:6b:2e:94:7e:43:77:
                    39:06:d2:4f:11:c0:c4:17:e5:eb:d6:10:a5:2c:fa:
                    4c:f1:50:35:59:59:2b:fa:b5:22:26:3f:0a:ff:f2:
                    f9:c4:d7:e2:67:5d:bf:b5:c1:cc:6b:77:31:e9:de:
                    95:b0:76:53:47:f7:1f:fe:c4:5b:c1:a7:fd:c4:fc:
                    61:d3:ea:b5:28:48:e5:d5:96:a0:11:ed:0b:00:a2:
                    42:c9:fa:94:26:89:f5:37:db:0a:9a:f8:95:e8:a6:
                    35:8a:68:33:90:c2:22:10:ad:65:3a:95:5f:64:1f:
                    6f:43:88:b2:1c:f8:29:9e:51:6b:e4:2d:8c:3e:39:
                    90:f7:31:8e:32:f8:0f:cf:3e:b4:7a:c6:f3:27:17:
                    a3:4e:3c:7c:27:07:3d:68:fc:5e:9c:87:86:74:ea:
                    22:32:d5:aa:93:e4:d4:78:23:d2:88:0f:e3:8f:05:
                    8c:54:b8:95:29:eb:c2:0a:fc:26:20:ca:52:ff:ce:
                    75:6b:29:82:d6:67:06:0b:49:53:37:0d:7e:cf:1c:
                    7e:88:90:8d:7a:e7:99:fc:9f:d7:5c:e2:1f:73:19:
                    cc:27:ba:31:6f:82:40:b0:cb:8a:d2:95:f4:6e:72:
                    78:b6:02:f5:f4:0b:b6:60:32:fb:3f:34:66:f2:a4:
                    12:c5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:67:FD:88:20:14:27:98:C7:09:D2:25:19:BB:E9:51:11:63:75:50:62
                  URI:http://crl3.digicert.com/TERENASSLCA3.crl
...
    Signature Algorithm: sha256WithRSAEncryption
         a3:aa:9b:c3:04:c3:5c:64:32:9c:8f:08:31:89:15:8a:52:19:
         fb:02:e9:dd:ab:59:3e:9e:d8:b8:52:b2:8d:df:5a:29:dc:2b:
         c0:01:7d:96:87:5c:a7:01:7e:26:c9:3b:be:01:d3:9c:71:62:
         e3:e5:a2:ce:5d:ee:59:b5:ed:20:d8:80:27:ac:af:f5:6a:73:
         79:35:d2:c5
```

Napad tablicama s unaprijed izračunatim sažecima

- *engl. rainbow table*
- za najčešće korištene zaporke se unaprijed izračunaju sažeci
- zapisi u datoteci sa zaštićenim lozinkama se uspoređuju s unaprijed izračunatim sažecima
- 7 najčešće korištenih zaporki:

	2018.	2021.	2023.	2025.
1.	123456	123456	123456	123456
2.	password	123456789	password	111111
3.	123456789	12345	123456789	admin
4.	12345678	qwerty	12345	qwerty
5.	12345	password	12345678	password
6.	111111	12345678	qwerty	123456789
7.	1234567	111111	1234567	123123

Zaključak o funkcijama sažimanja

- kolizije su bezopasne sve dok izgledaju kao slučajan niz
- međutim, gubi se povjerenje u certifikate
  - protokoli koji koriste sažetak slučajnog simetričnog ključa nisu više sigurni
- problem nevidljivih podataka u Word dokumentu ili slučajnih nizova u slikama
- rješenje:
  - koristiti obične tekstualne datoteke ili potpisati sažetu datoteku (kao što PGP koristi *zip*)
  - koristiti novi algoritam sažimanja SHA-3