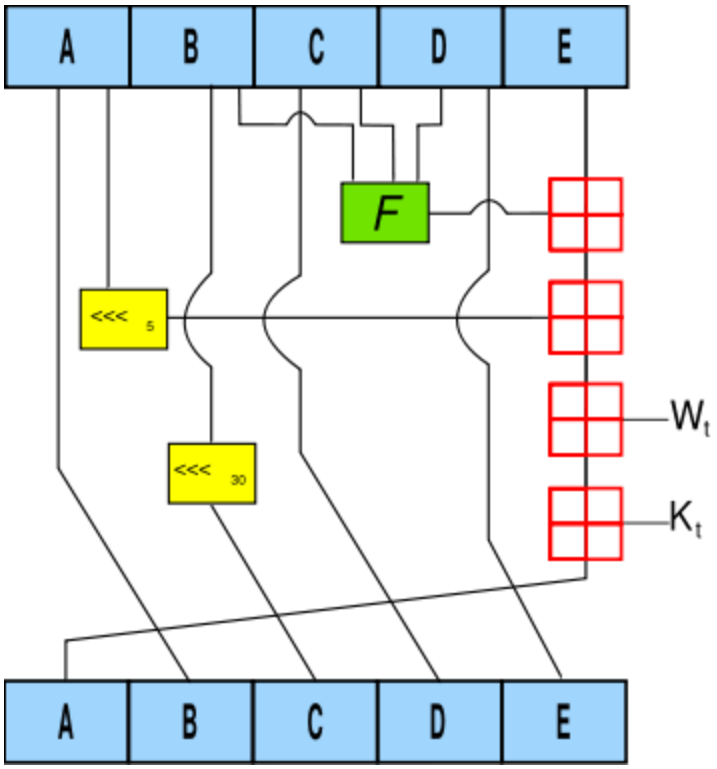
Zgoščevalne funkcije ('*Hash functions*')

- So namenjene pridobivanju izvlečka ali prstnega odtisa sporočila:
  - Preslikajo poljubno dolgo sporočilo v blok podatkov končne dolžine.
- So enosmerne funkcije in vsaka sprememba čistopisa spremeni tudi prstni odtis sporočila.
- Uporabljajo se za digitalne podpise:
  - Pošiljatelj s pomočjo zgoščevalne funkcije naredi prstni odtis sporočila
  - Prstni odtis sporočila nato šifrira s svojim zasebnim ključem
  - Sprejemalec dešifrira prstni odtis originalnega sporočila z javnim ključem pošiljatelja
  - Tudi sprejemalec z zgoščevalno funkcijo naredi prstni odtis prejetega sporočila
  - Če se oba zgoraj navedena odtisa ujemata:
    - je sporočilo verodostojno
    - potrjena je identiteta pošiljatelja
    - pošiljatelj ne more zanikati sporočila
- Verjetnost, da najdemo sporočilo z enakim prstnim odtisom mora biti zelo majhna. Slednje dosežemo z zadosti dolgim ključem.

SHA1 – Secure Hash Algorithm

- Razvit s strani *National Security Agency*.
- Sporočilo razdelimo na bloke dolžine 512 bitov.
- Rezultat zgoščevalne funkcije je 160-bitov dolg prstni odtis.
- Računanje prstnega odtisa se ponavlja za vsak blok. Pri tem se upošteva prstni odtis prejšnjega bloka.
- Računanje prstnega odtisa vsakega bloka poteka v ciklih (t=80). Pri vsakem ciklu se upošteva prejšnje stanje sistema.



Slika 1: En cikel izračuna zgoščevalne funkcije.

- A, B, C, D in E so 32-bitov dolge besede -> trenutno stanje sistema.
- F je nelinearna funkcija, ki se spreminja.
- $<<_n$ pomeni rotacijo bitov za n v levo; n se spreminja.
- W_t je razširjeno sporočilo koraka t.
- K_t je konstanta cikla t
- $\boxplus$ pomeni seštevanje po modulu 2^{32}.

Naloge:

1. V programskem okolju Matlab preučite in dopolnite funkcijo fnSHA1 za računanje prstnih odtisov niza znakov *hash=SHA1(vhNizZnakov)*
   a. Vhodni niz znakov pretvorite v niz bitov.
   b. Vhodni niz bitov dopolnite:
      i. Nizu bitov dodajte bit '1'
      ii. Dodajte 0 <= k < 512 bitov '0' tako, da bo končni niz dolg 448 po modulu 512.
      iii. Nizu bitov dodajte dolžino originalnega sporočila v bitih.

```
block_temp = [ini, '1', num2str(zeros(mod(448-1-lM*8,512),1))', dec2bin(lM*8,64)];
```

   c. Pridobljeni niz bitov razdelite na bloke velikosti 512:

```
nb=length(block_temp)/512;

block = reshape(block_temp,512,nb)';
```

   d. Postavite začetno vrednost prstnega odtisa:

```
H = ['67','45','23','01';
     'ef','cd','ab','89';
     '98','ba','dc','fe';
     '10','32','54','76';
     'c3','d2','e1','f0']
```

   e. Postavite ustrezno vrednost konstante K cikla:
   t… zaporedna številka cikla
   za 1<=t<=20
   K=['5A','82','79','99'];
   za 20<t<=40
   K=['6E','D9','EB','A1'];
   za 40<t<=60
   K=['8F','1B','BC','DC'];
   za 60<t<=80
   K=['CA','62','C1','D6'];

   f. Za vsak cikel izračunajte končno vrednost vsote T:

```
T = mod(T1+T2+T3+T4+T5,2^32);
```

g. Ustrezno postavite novo stanje sistema (A, B, C, D in E) za vsak cikel računanja zgoščevalne funkcije posameznega bloka:

```
E = D;
D = C;
C = cls(B,30);
B = A;
A = dec2bin(T,32);
```

h. Za vsak blok podatkov izračunajte pripadajoč prstni odtis:

```
H = izracunaNovHash(H,A,B,C,D,E);
```

2. Preizkusite delovanje algoritma:
   a. Izračunajte prstni odtis za nekaj poljubnih nizov znakov.
   b. Prstni odtis praznega niza je:

      _____
      _____
      _____
      _____
      _____

   c. Končna dolžina prstnega odtisa je _____ bitov.

3. Funkcijo *SHA1* uporabite za računanje prstnih odtisov datotek:
   a. Določite vhodno in izhodno datoteko:

```
fname=input('Ime vhodne datoteke (v ASCII formatu)? ','s');
hash_foutname=input('Ime izhodne datoteke za SHA1 rezultat?','s');
```

   b. Preberite vhodne podatke:

```
fid=fopen(fname);
Mdec = fread(fid);
fclose(fid);
```

4. Preverite delovanje funkcije *SHA1* za računanje prstnih odtisov datotek:

   a. Prstni odtis datoteke test.txt je:

   _____
   _____
   _____
   _____
   _____

   b. V datoteki test.txt spremenite en bit vsebine. Prstni odtis spremenjene datoteke test.txt je :

   _____
   _____
   _____
   _____
   _____

   c. V datoteki test.txt dodajte poljubno vrstico. Prstni odtis spremenjene datoteke test.txt je:

   _____
   _____
   _____
   _____
   _____

5. Ugotovite kakšna je distribucija prstnih odtisov vseh datotek shranjenih na C disku računalnika.