Administrivia: HW groups?
new students?

Outline:

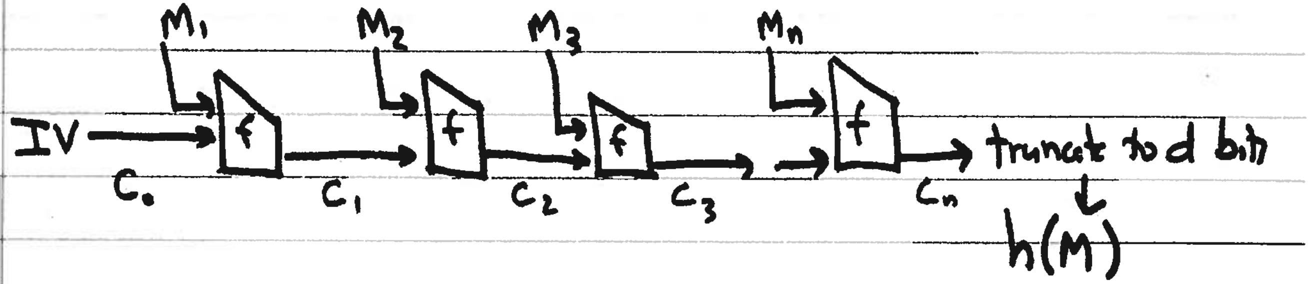
□ Merkle-Damgard } L2.6-L2.7 for 2/9/09
□ MD5 }
□ MD6 (crypto slides)

Construction ("Merkle-Damgard" style")

- Choose output size d (e.g. $d=160$)
- Choose chaining variable size c (e.g. $c=160$) (better if $c \geq 2d$!)
- Choose block size b for message
- Design "compression fn" f (OW, CR, PR, NM, TCR, ...)

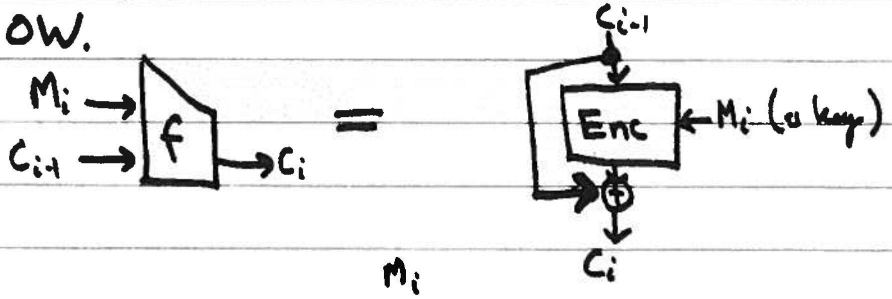
  $f: \{0,1\}^c \times \{0,1\}^b \to \{0,1\}^c$
- Choose c-bit IV (initialization vector)
- Given message, add both 10^*-bits & "length of m" $|m|$ so that m's new length is multiple of b bits

  now $M = M_1 M_2 \cdots M_n$ (n b-bit blocks)

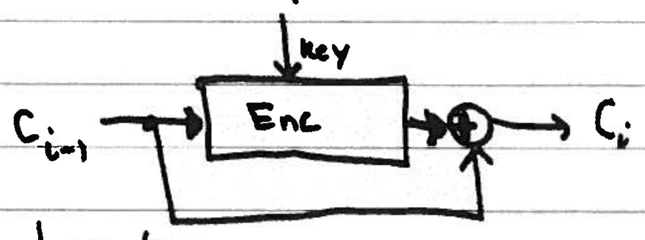


- Like "mode of operation" for encryption algorithm.
- IV is arbitrary, but fixed.
- Thm: If f is CR, then so is h.

  Pf: Work backwards through chain from h-collision to find f-collision.
- Thm: Same for OW.
- Common pattern:



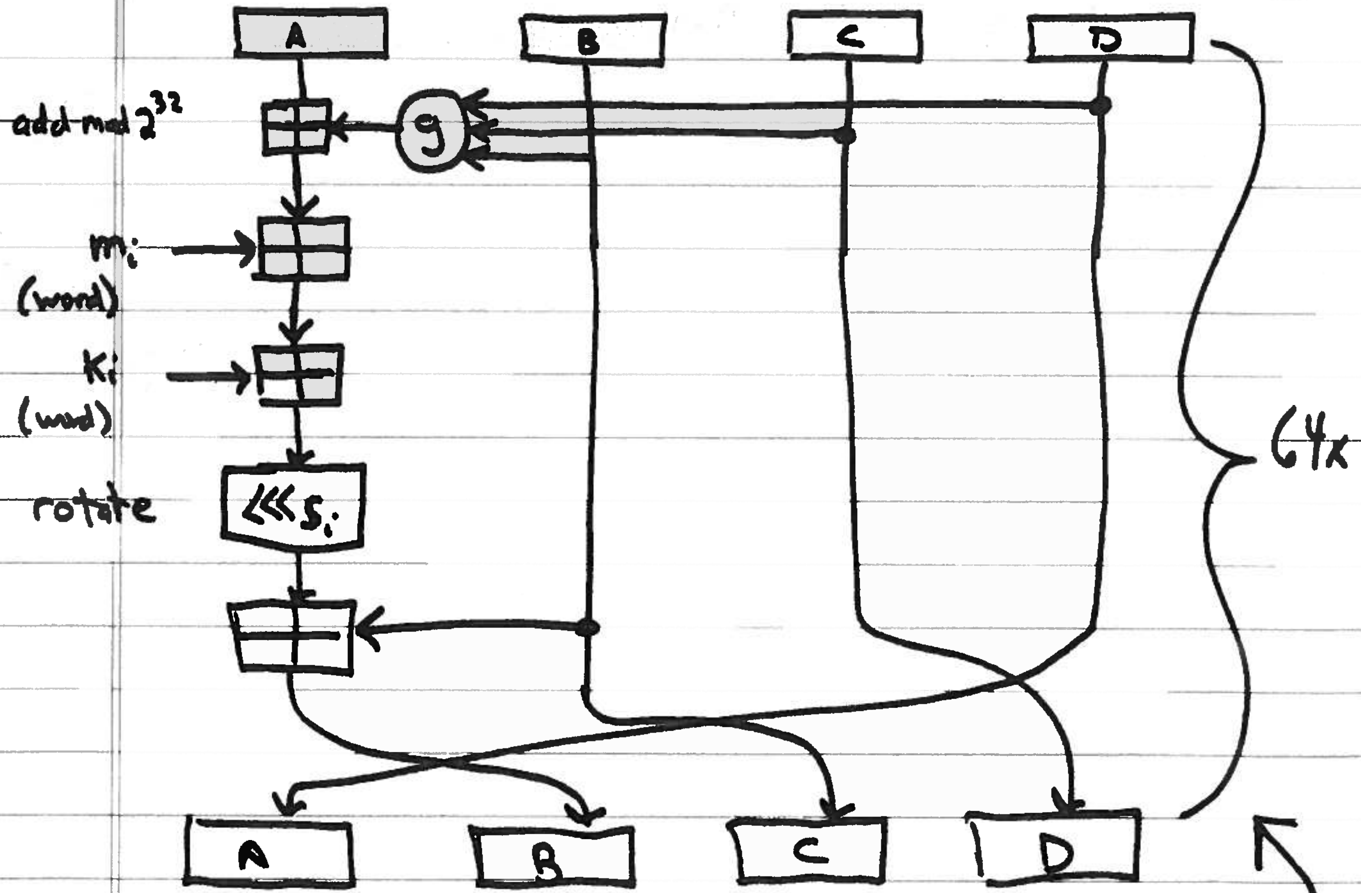
or



But AES etc. are hard to change keys...

Typical compression function (MD5):

- chaining variable & output are 128 bits = 4 x 32
- IV = fixed value
- 64 rounds; each modifies state (in reversible way) based on selected message ~~block~~ word
- message block b=512 bits considered as 16 32-bit words
- uses end-around XOR too around entire compression fn (as above)



Xiayun Wang discovered how to make collisions for MD4, MD5,...
("Differential cryptanalysis")

SHA-3 contest now underway...

$$g(x,y,z) = \begin{cases} xy \vee \bar{x}z \\ xz \vee y\bar{z} \\ x \oplus y \oplus z \\ y \oplus x\bar{z} \end{cases}$$ depending on round