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 $c > 2d$)
- Choose block size $b$ for message
- Design "compression fn" $f$
  \[ f : \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c \]
- Choose $c$-bit IV (initialization vector)
- Given message, add both $10^b$ bits & "length of $m$" \(|m|\)
  so that $m$'s new length is multiple of $b$ bits
  now $M = M_1, M_2, \ldots, M_n$ (in $b$-bit blocks)

\[
\begin{array}{cccccc}
\text{IV} & \rightarrow & f & \rightarrow & f & \rightarrow & f & \rightarrow & \text{truncate to } d \text{ bit} \\
& & C_0 & & C_1 & & C_2 & & C_3 & & C_n & & \downarrow h(M)
\end{array}
\]

- 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: $M_i \rightarrow f \rightarrow C_i$

\[
\begin{array}{c}
C_i = \text{Enc}(M_i \oplus \text{key})
\end{array}
\]

or

\[
\begin{array}{c}
C_i = \text{Enc}(\text{key} \oplus C_{i-1})
\end{array}
\]

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 reverse 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 collision for MD4, MD5...
("Differential cryptanalysis")

SHA-3 contest now underway...

\[
g(\langle x, y \rangle) = \begin{cases} 
xy & x \neq 0, y \neq 0 \\
x^2 + y^2 & x \neq y, y = 0 \\
xy & x = y, x \neq 0 \\
0 & x = 0, y = 0 \\
\end{cases}
\] depending on round.