Secure Hash Algorithm (SHA)

• Pad message so it can be divided into 512-bit blocks, including a 64 bit value giving the length of the original message.
• Process each block as 16 32-bit words called $W(t)$ for $t$ from 0 to 15.
• Expand from these 16 words to 80 words by defining as follows for each $t$ from 16 to 79:
  – $W(t) := W(t-3) \oplus W(t-8) \oplus W(t-14) \oplus W(t-16)$
• Constants $H_0$, …, $H_5$ are initialized to special constants
• Result is final contents of $H_0$, … , $H_5$
for each 16-word block begin

A := H0; B := H1; C := H2; D := H3; E := H4
for I := 0 to 19 begin
    TEMP := S(5,A) + ((B ∧ C) ∨ (¬B ∧ D)) + E + W(I) + 5A827999;
    E := D; D := C; C := S(30,B); B := A; A := TEMP
end
for I := 20 to 39 begin
    TEMP := S(5,A) + (B ⊕ C ⊕ D) + E + W(I) + 6ED9EBA1;
    E := D; D := C; C := S(30,B); B := A; A := TEMP
end
for I := 40 to 59 begin
    TEMP := S(5,A) + ((B ∧ C) ∨ (B ∧ D) ∨ (C ∧ D)) + E + W(I) + 8F1BBCDC;
    E := D; D := C; C := S(30,B); B := A; A := TEMP
end
for I := 60 to 79 begin
    TEMP := S(5,A) + (B ⊕ C ⊕ D) + E + W(I) + CA62C1D6;
    E := D; D := C; C := S(30,B); B := A; A := TEMP
end
H0 := H0+A; H1 := H1+B; H2 := H2+C; H3 := H3+D; H4 := H4+E
end
Attacks against SHA-1

• In early 2005, Rijmen and Oswald published an attack on a reduced version of SHA-1 (53 out of 80 rounds)
  – finds collisions with a complexity of fewer than $2^{80}$ operations.
• In February 2005, an attack by Wang, Yin, and Yu was announced.
  – Finds collisions in the full version of SHA-1, requiring fewer than $2^{69}$ operations (brute force would require $2^{80}$.)
• In August 2005, same group lowered the threshold to $2^{63}$.
• Currently best known collision attacks: $2^{57}$