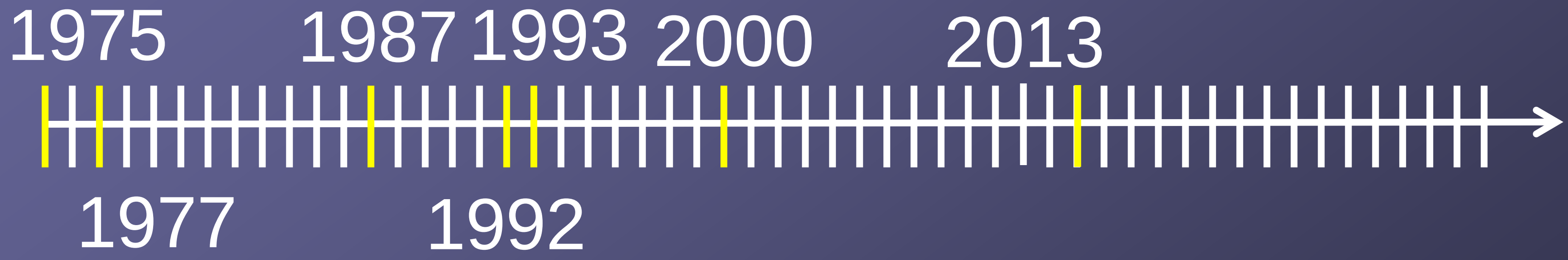
DTTF/NB479: Dszquphsbqiz Day 14

- Announcements:
  - Homework 3 due now
  - Homework 4 posted
- Today:
  - Attacks on DES
- Questions?

DES has been showing signs of weakness from the beginning



Only 2^{56} = 72,057,594,037,927,936 keys, so it was brute forced using parallelism

- *1997:* DES Challenge issued. $10K prize
  - Found after 5 months, searching ___% of keyspace
- *1998:* DES Challenge II
  - Down to 39 days, 85% of keyspace!
- Also in 1998…

DES Cracker used a mixture of software and specialized hardware

- Budget of only $200,000 1998 dollars
  - vs $20,000,000 1977 dollars

- Result?

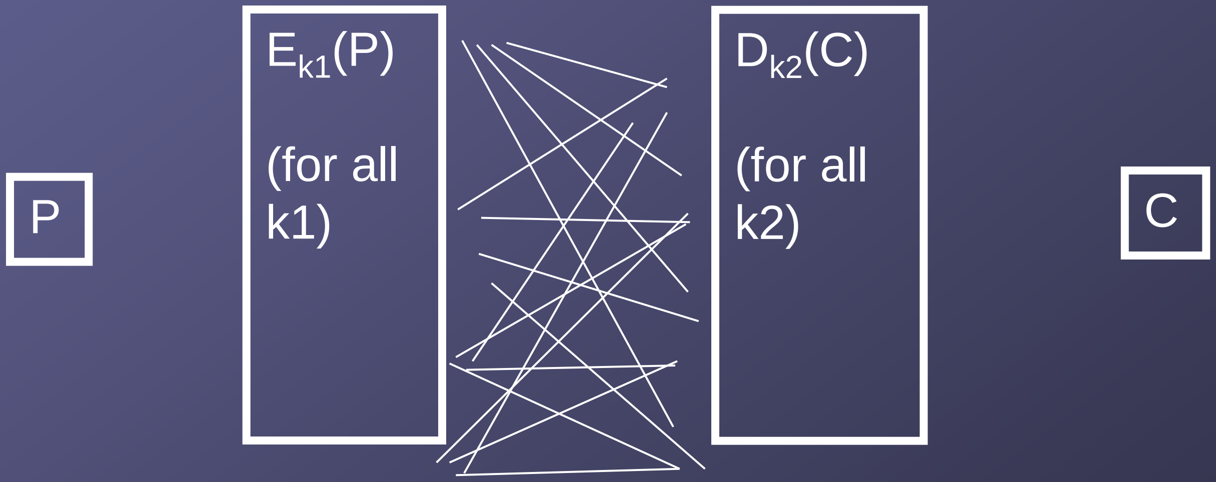
Post-DES

- Brute force attacks that take O(N) DES computations are now reasonable.
  - N is size of keyspace = 2^{56}
- Can we just double encrypt to get $O(N^2)$ computations?
  - Use k1, k2
  - $C = E_{k2}(E_{k1}(P))$, so $P = D_{k1}(D_{k2}(C))$?

Meet-in-the-middle attack

Assume k completely determines E_k and D_k

Know P and C = $E_{k2}(E_{k1}(P))$



P

$E_{k1}(P)$

(for all k1)

$D_{k2}(C)$

(for all k2)

C

Time complexity?
O(n) DES computations, O(n^2) comparisons O(n) memory

Triple-DES?

Type	DES computations	Comparisons	Memory	Brute force DES
Double $C=E_{k2}(E_{k1}(P))$	O(N)	$O(N^2)$	O(N)	$O(N^2)$
Triple1 $C=E_{k3}(E_{k2}(E_{k1}(P)))$				
Triple2 $C=E_{k1}(E_{k2}(E_{k1}(P)))$				
Triple3 $C=E_{k2}(E_{k1}(E_{k1}(P)))$				

Describe attacks on triple 1-3, fill out chart, and order by level of security

Triple-DES?

Type	DES computations	Comparisons	Memory	Brute force DES
(3) Double $C=E_{k2}(E_{k1}(P))$	$O(N)$	$O(N^2)$	$O(N)$	$O(N^2)$
(1) Triple1 $C=E_{k3}(E_{k2}(E_{k1}(P)))$	$O(N^2)$	$O(N^3)$	$O(N^2)$	$O(N^3)$
(2) Triple2 $C=E_{k1}(E_{k2}(E_{k1}(P)))$				
(3) Triple3 $C=E_{k2}(E_{k1}(E_{k1}(P)))$				

Describe attacks on triple 1-3, fill out chart, and order by level of security

Triple-DES?

Type	DES computations	Comparisons	Memory	Brute force DES
(3) Double $C=E_{k2}(E_{k1}(P))$	O(N)	$O(N^2)$	O(N)	$O(N^2)$
(1) Triple1 $C=E_{k3}(E_{k2}(E_{k1}(P)))$	$O(N^2)$	$O(N^3)$	$O(N^2)$	$O(N^3)$
(2) Triple2 $C=E_{k1}(E_{k2}(E_{k1}(P)))$	$O(N^2)$	$O(N^3)$	$O(N^2)$	$O(N^2)$
(3) Triple3 $C=E_{k2}(E_{k1}(E_{k1}(P)))$				

Describe attacks on triple 1-3, fill out chart, and order by level of security

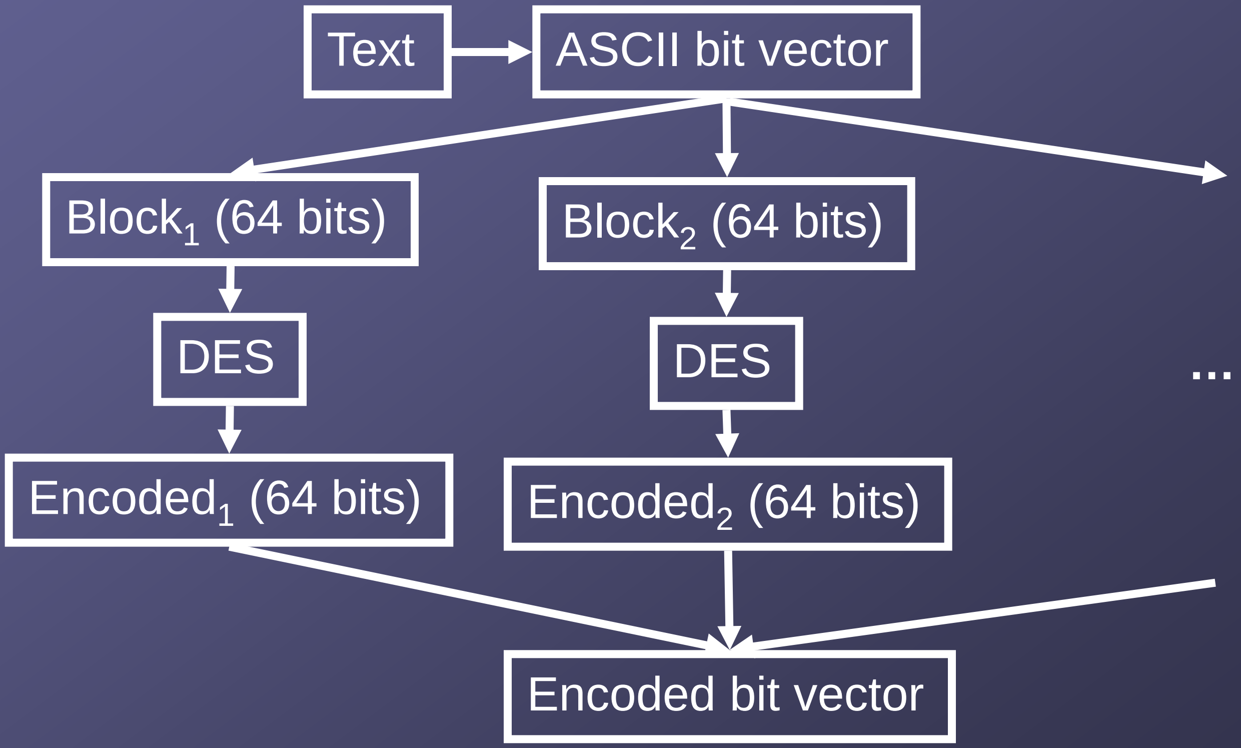
Triple-DES?

Type	DES computations	Comparisons	Memory	Brute force DES
(3) Double $C=E_{k2}(E_{k1}(P))$	$O(N)$	$O(N^2)$	$O(N)$	$O(N^2)$
(1) Triple1 $C=E_{k3}(E_{k2}(E_{k1}(P)))$	$O(N^2)$	$O(N^3)$	$O(N^2)$	$O(N^3)$
(2) Triple2 $C=E_{k1}(E_{k2}(E_{k1}(P)))$	$O(N^2)$	$O(N^2)$	$O(N^2)$	$O(N^2)$
(3) Triple3 $C=E_{k2}(E_{k1}(E_{k1}(P)))$	$O(N)$	$O(N^2)$	$O(N)$	$O(N^2)$

Describe attacks on triple 1-3, fill out chart, and order by level of security

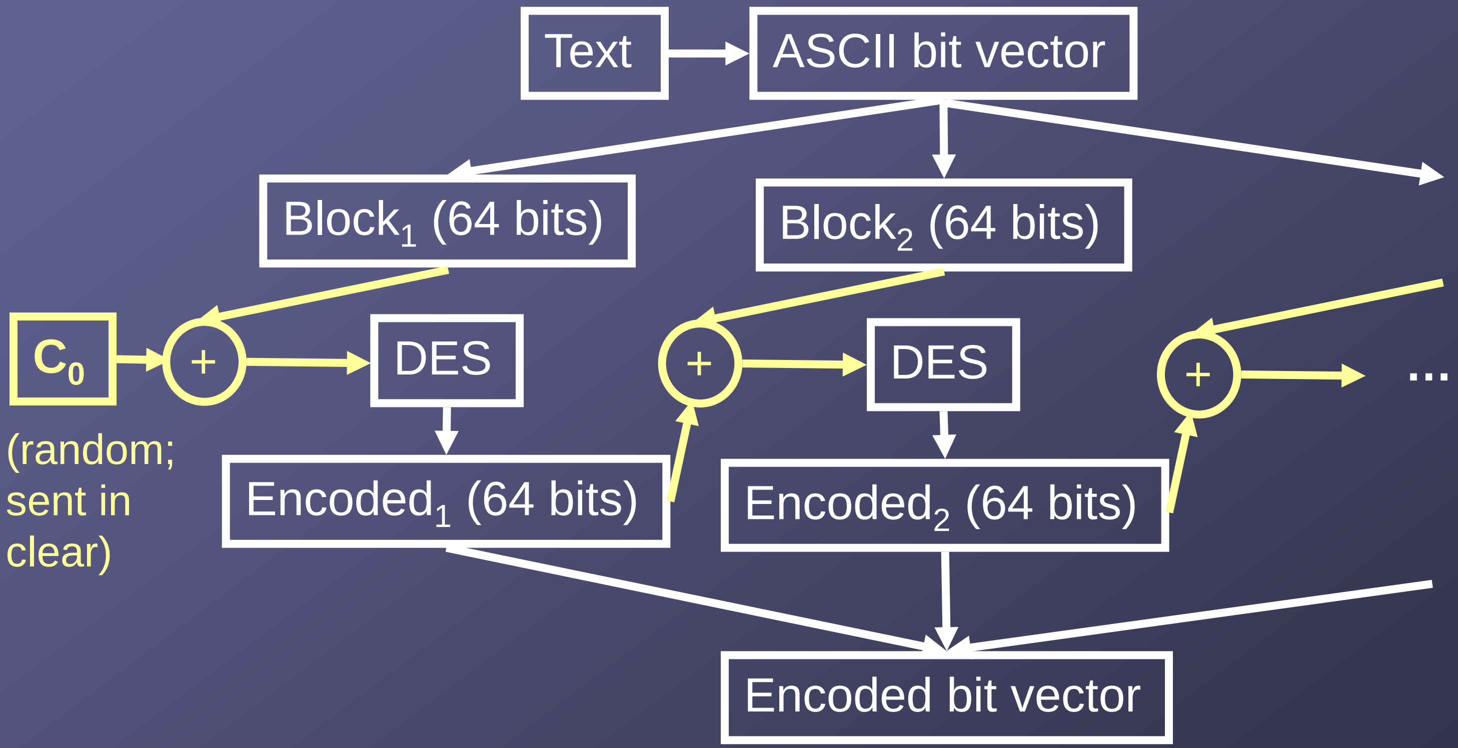
DES Modes of Operation

- *Electronic codebook:* Each block is encoded independently



DES Modes of Operation

- *Cipher-block chaining:* Each plaintext block is XOR'ed with the previous ciphertext before going into DES
  - We will do a simpler version of this in HW4 (set $C_0 = 0$)


Text
ASCII bit vector
Block_1 (64 bits)
Block_2 (64 bits)
C_0
+
DES
+
DES
+
…
(random; sent in clear)
Encoded_1 (64 bits)
Encoded_2 (64 bits)
Encoded bit vector

DES Modes of Operation

- Others:
  - *Cipher feedback:* similar, but 64-bit blocks overlap, giving k bits at a time (like 8 for 1 character at a time)
    - Uses pseudorandom bits like LFSR
  - *Output feedback:* similar but helps catch errors before propagate.
  - *Counter*: Some output can be computed independently, so better for parallelizing
- I trust you could implement these if needed. Not part of HW4…

HW4: DES Implementation

- Encryption and decryption.
- Cipher-block chaining to prevent speedups due to embarrassing parallelism
- Correctness:
  - Can use one to test the other.
- Efficiency:
  - In addition, it’d be nice to use a language that’s closer to the hardware for efficiency, like C or non-OO Java.
  - Part of your grade will depend on this
  - There will also be a competition to see whose implementation is quickest!

Questions so far on DES?