CIS 3362 9/27/23

Quiz 2

Avg Q1 = 66 %, Avg Q2 = 51 %

Q3 avg 30 pts

asked class memorize formula 2×2 mat inv.
* EEA (5 pts)

Q6 avg 27 %

Coded in class WCD

```
for (int i = 0; i < n; i++)
    invperm[perm[i]] = i;
```

perm[i]: old output; i: old input

f

a → c
w → a
b → q

f^{-1}

a ∈ c
w ∈ a
b ∈ q

DES

Data Encryption Standard

Want govt standard private key encryption

for computers keys are going to be bitstrings

block encryption

We specify private key algorithms on a single block

Lucifer (orig at IBM) → winner → NSA modifications → DES

? look up

Govt standard 1970s → late 1990s or 2000s

Input Block Plaintext is 64 bits

Key 56 bits w/ 8 parity bit (write 64 bits but only 56 are spec the key)

Cipher in Rounds

16 Rounds

1. Input = ~~L_0R_0~~ X (64 bits

   $IP(X) = L_0R_0$ (left 32 bits, right 32 bits)

2. Run 16 rounds

   for (i=1; i<=16; i++) {

   $L_i = R_{i-1}$

   $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ (XOR)

   K_1 through K_{16} are 16 round keys each 48 bits

   }

3. Cipher $= IP^{-1}(R_{16}L_{16})$

function → 32 bits (old left), 48 bits round key

$f(A, J)$

1. Calculate $E(A)$ 32 bits → 48 bits
2. $B = E(A) \oplus J = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$ (6 bits each)
3. for $(i=1; i \leq 8; i++)$
   $C_i = S_i(B_i)$ [Apply S-box i to B_i to obtain C_i]
   input S-box 6 bits → output 4 bits
4. Output $P(C_1 C_2 C_3 \ldots C_8)$
   ↙ another perm matrix