UCI University of California, Irvine

MITRE eCTF 2023-24

LAB 1 Workshop

Jinyao Xu (jinyaox@uci.edu)

SAT Problem (Karp's 21 NP Complete)

F=(a V b)(a V -b)(-a V c)(-c V b) --> abc=111

F=(a V b)(a V -b)(-a V c)(-c V -a) --> NO SOLUTION

- *Decision Problem:* Is there an assignment to make it return True?
- *Dual Problem:* Find an assignment to make it return True?
- Both are NP-Complete, solvable with brute force.

Proof: 1. Show it's NP

2. Show it's NP-Hard by reducing Circuit-SAT to it

LAB ACTIVITY

LAST TIME:

- **Confirmed Communication and database structure**
- **Issue Remaining: Generate Random Number?**
- **Some Code Examples we can use:**

https://github.com/Jinyaox/TIVA_C_Secure_lib?search=1

Plain text = P

Encrypted text = C

Jet: $[k_{p_1}, k_{p_2}, k_{p_3}]$

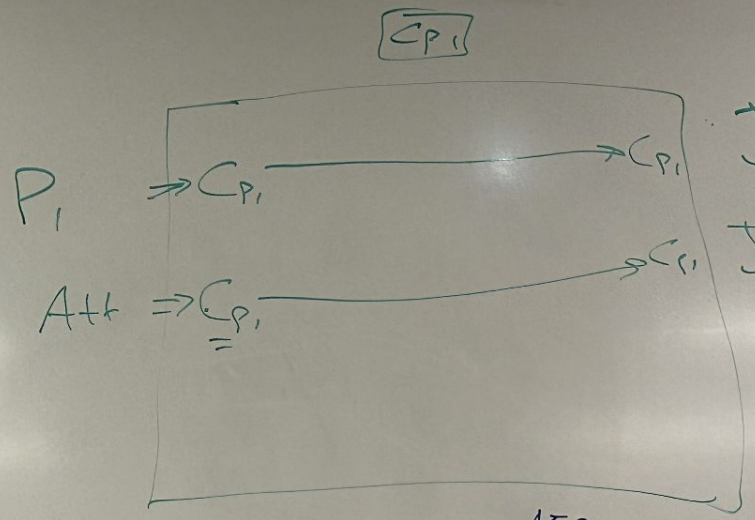
$P_1 : k_{p_1}$

$P_2 : k_{p_2}$

$P_3 : k_{p_3}$

$E(P \cdot k_{p_1} \cdot N) = C_{p_1}$

$D(C \cdot k_{p_1}) = P_{p_1}$



AES: 2 ms.

1. Goal 1 : Ciphertext indistinguishability.

CSV file.

- py. load procs.
- py. generate nonce.
- py. validate
- py. send out.

Interval: 0.1 sec.

100 ms.

JET

Pilot

- EEPROM STORE info. AES private key
- [Recieve Encrypt Send.] = Button push

K_{P1} → 3 →

← C_{P1}

$D_{K1}(C_{P1}) = 3$

K_{P1} UART Rx AES Lib UART Tx

$E_{K1}(3) = C_{P1}$