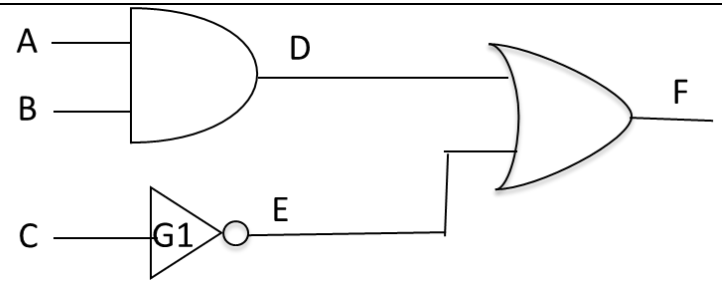
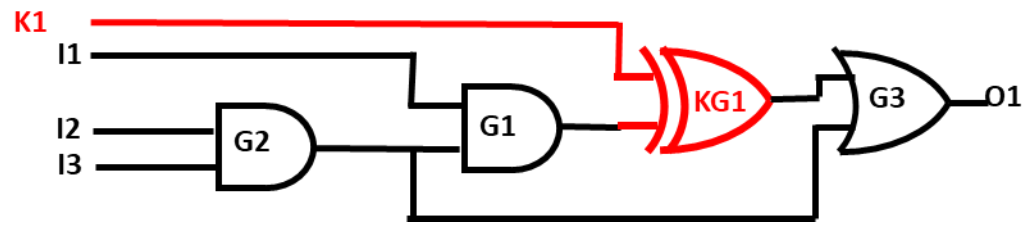
SAT 101: Deciphering SAT Attack on Computer Chips

ACTIVITY 01: CNF from a circuit

Objective: Learn to use Tseytin transformation to construct CNF formulas from gate-level circuits.

Question: For the circuit(s) given below, generate the CNF formula. Use the diagram at the bottom of the page for generating clauses for individual gates.

Practice Circuit	**Test Circuit**
	
Practice Circuit CNF	**Test Circuit CNF**

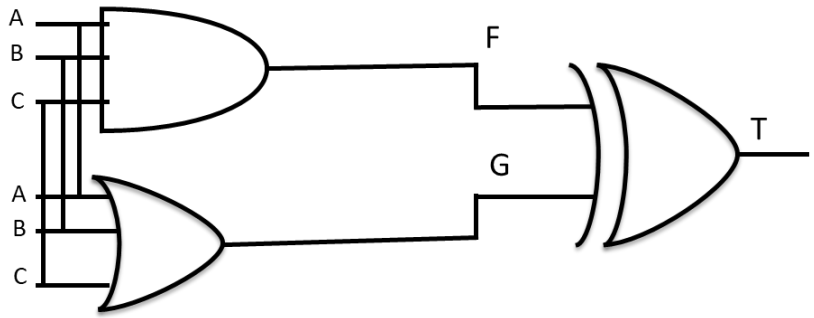
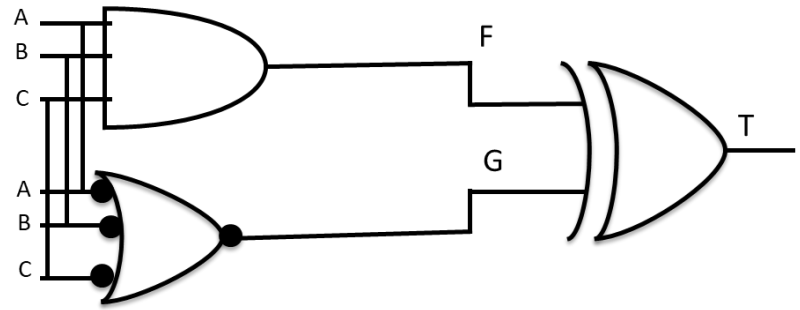
Type	Operation	CNF sub-expression
AND	$C = A \cdot B$	$(\overline{A} \vee \overline{B} \vee C) \wedge (A \vee \overline{C}) \wedge (B \vee \overline{C})$
NAND	$C = \overline{A \cdot B}$	$(\overline{A} \vee \overline{B} \vee \overline{C}) \wedge (A \vee C) \wedge (B \vee C)$
OR	$C = A + B$	$(A \vee B \vee \overline{C}) \wedge (\overline{A} \vee C) \wedge (\overline{B} \vee C)$
NOR	$C = \overline{A + B}$	$(A \vee B \vee C) \wedge (\overline{A} \vee \overline{C}) \wedge (\overline{B} \vee \overline{C})$
NOT	$C = \overline{A}$	$(\overline{A} \vee \overline{C}) \wedge (A \vee C)$
XOR	$C = A \oplus B$	$(\overline{A} \vee \overline{B} \vee \overline{C}) \wedge (A \vee B \vee \overline{C}) \wedge (A \vee \overline{B} \vee C) \wedge (\overline{A} \vee B \vee C)$
XNOR	$C = \overline{A \oplus B}$	$(\overline{A} \vee \overline{B} \vee C) \wedge (A \vee B \vee C) \wedge (A \vee \overline{B} \vee \overline{C}) \wedge (\overline{A} \vee B \vee \overline{C})$

SAT 101: Deciphering SAT Attack on Computer Chips

ACTIVITY 02: Miter Circuit Operation & Differing Input Pattern

Objective: Practice use of a miter circuit to compare two circuits.

Question: For the circuit(s) given below, check if an input pattern exists for which the miter circuit output is 1.

Practice Circuit	**Test Circuit**
	
Practice Circuit differing input patten	**Test Circuit differing input patten**

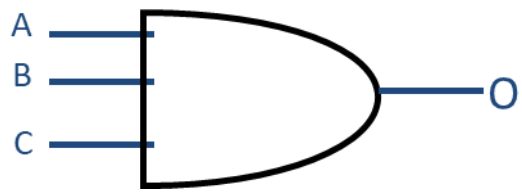
SAT 101: Deciphering SAT Attack on Computer Chips

ACTIVITY 03: Generate Distinguishing Input Pattern for a Locked circuit (Optional Activity)

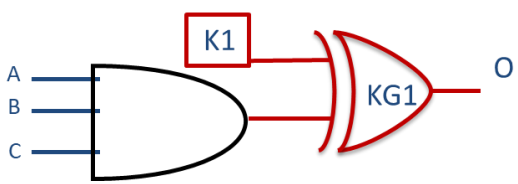
Objective: Practice use of a miter circuit to generate distinguishing input pattern for a locked circuit.

Question: For the circuit given miter circuit below, generate a DIP – distinguishing input pattern.

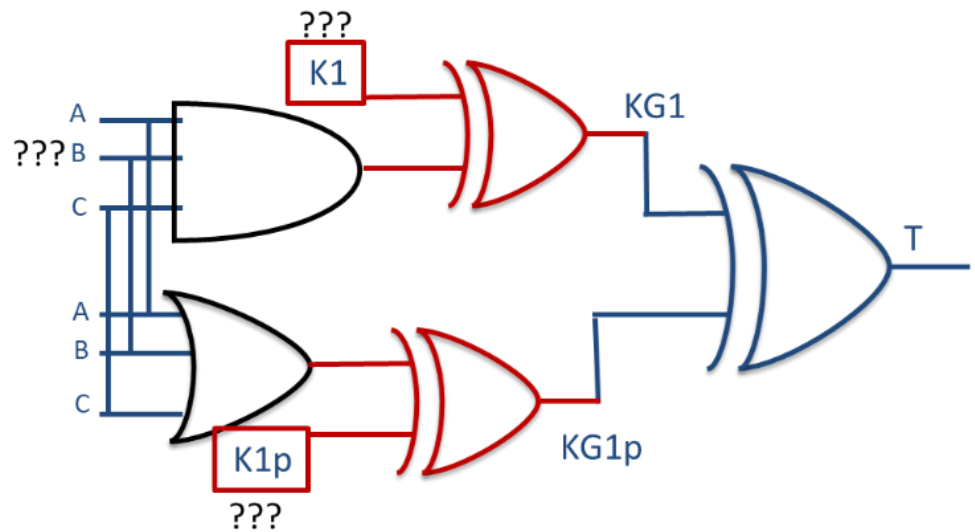
Original circuit



Locked circuit



Miter circuit



Distinguishing input pattern: