

Assignment 0

Due by Tuesday, February 11, at 11am

Submit a hardcopy of your solution at the beginning of class

Give a step-by-step explanation of how EASYCRYPT processes the proof script `ass0.ec`—which is listed below. Hint: run this script, step-by-step in Emacs (using Proof General to interact with EASYCRYPT), and explain what is happening at each point in time as clearly as you can.

```
lemma negb_or (a b : bool) :
  !(a  $\vee$  b)  $\Leftrightarrow$  !a  $\wedge$  !b.
proof.
split.
move => not_or.
split.
case a.
move => a_true.
simplify.
have contrad : a  $\vee$  b.
  left.
  trivial.
trivial.
trivial.
case b.
move => b_true.
simplify.
have contrad : a  $\vee$  b.
  right.
  trivial.
trivial.
trivial.
move => and_not.
elim and_not => a_false b_false.
case (a  $\vee$  b).
move => or.
elim or.
trivial.
trivial.
trivial.
qed.
```