PART A:

1. The more challenges that are universally possible, the lower chance the attacker will succeed in having a corresponding Nc. The size of Nr is less important, since the attacker is attempting to exploit Nc. Therefore, C should be the most secure design.

2. Do not allow the car to start unless the keys are inside or next to the car.

PART B:

a)

A -> I(B): A, N_a
I(B) -> A: B, N_b
A -> I(B): $N_{a,}$, {A, B, N_b}$_{Kab}$
...
I(B) -> A: {A, B, N_b}$_{Kab}$

b) Include a fresh K_{AB} to the encrypted content, then A must decypt it and re-encrypt using the fresh key, B can then expect to decrypt the message using the key it just sent.

c) Once the fresh key is known to A, a man-in-the-middle attack can intercept the new key. You could also add a timestamp to the encrypted content to check how old the delivered message is.

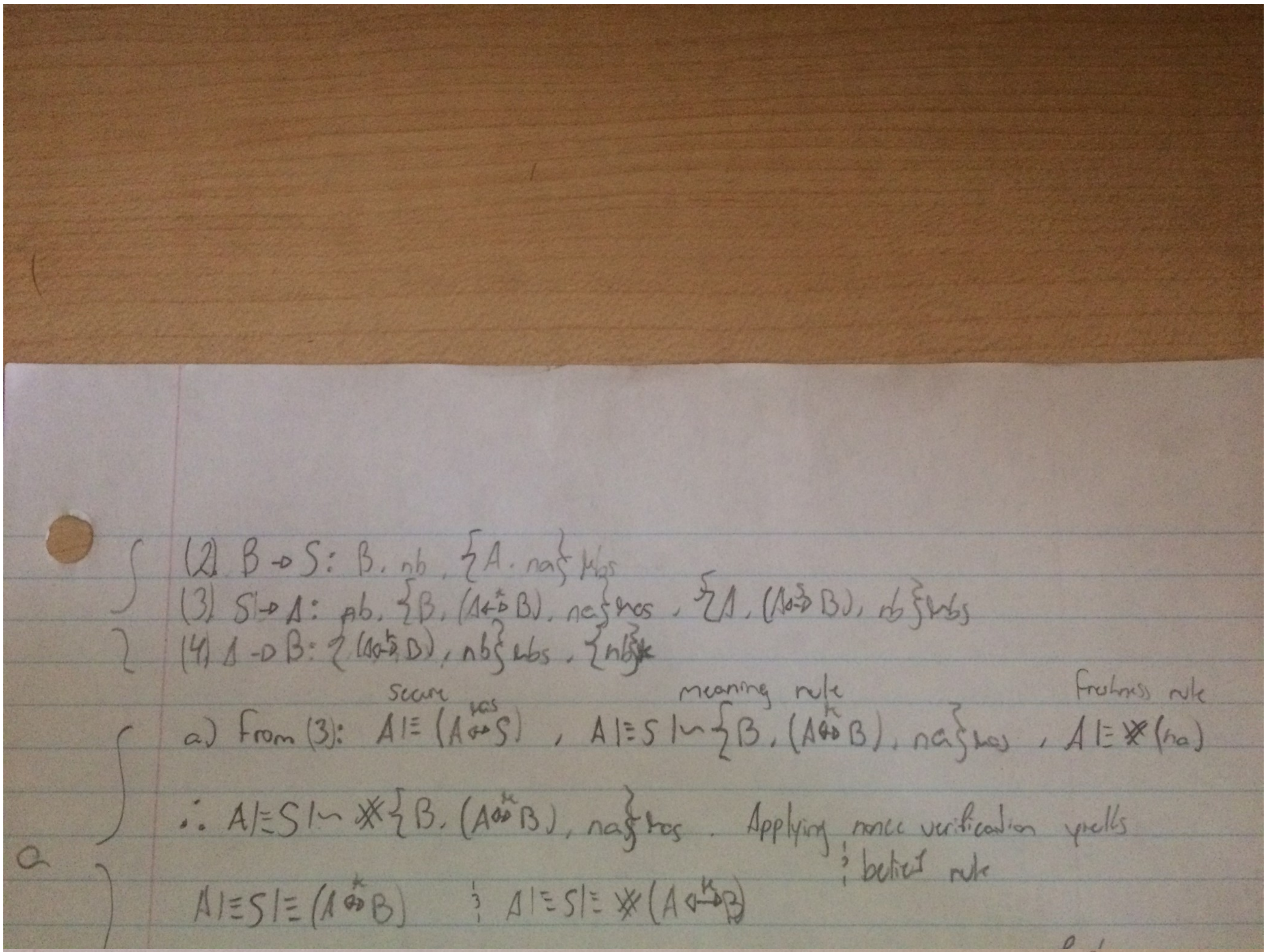
PART C:

a) (Diffie Hellmann Example) If P is a large enough number, finding what the shared secret is could take more than the lifetime of the universe. An eavesdropper cannot succeed despite knowing p and g.

b) A large enough shared secret is necessary to make this protocol secure.

c) The key in the second protcol is N_a NOR N_b, and therefore relies on both parties sending/not reading their nonce before decrypting the message.

PART D



(2) $B \rightarrow S: B, nb, \{A, na\}_{K_{bs}}$

(3) $S \rightarrow A: nb, \{B, (A \xleftrightarrow{K} B), na\}_{K_{as}}, \{A, (A \xleftrightarrow{K} B), nb\}_{K_{bs}}$

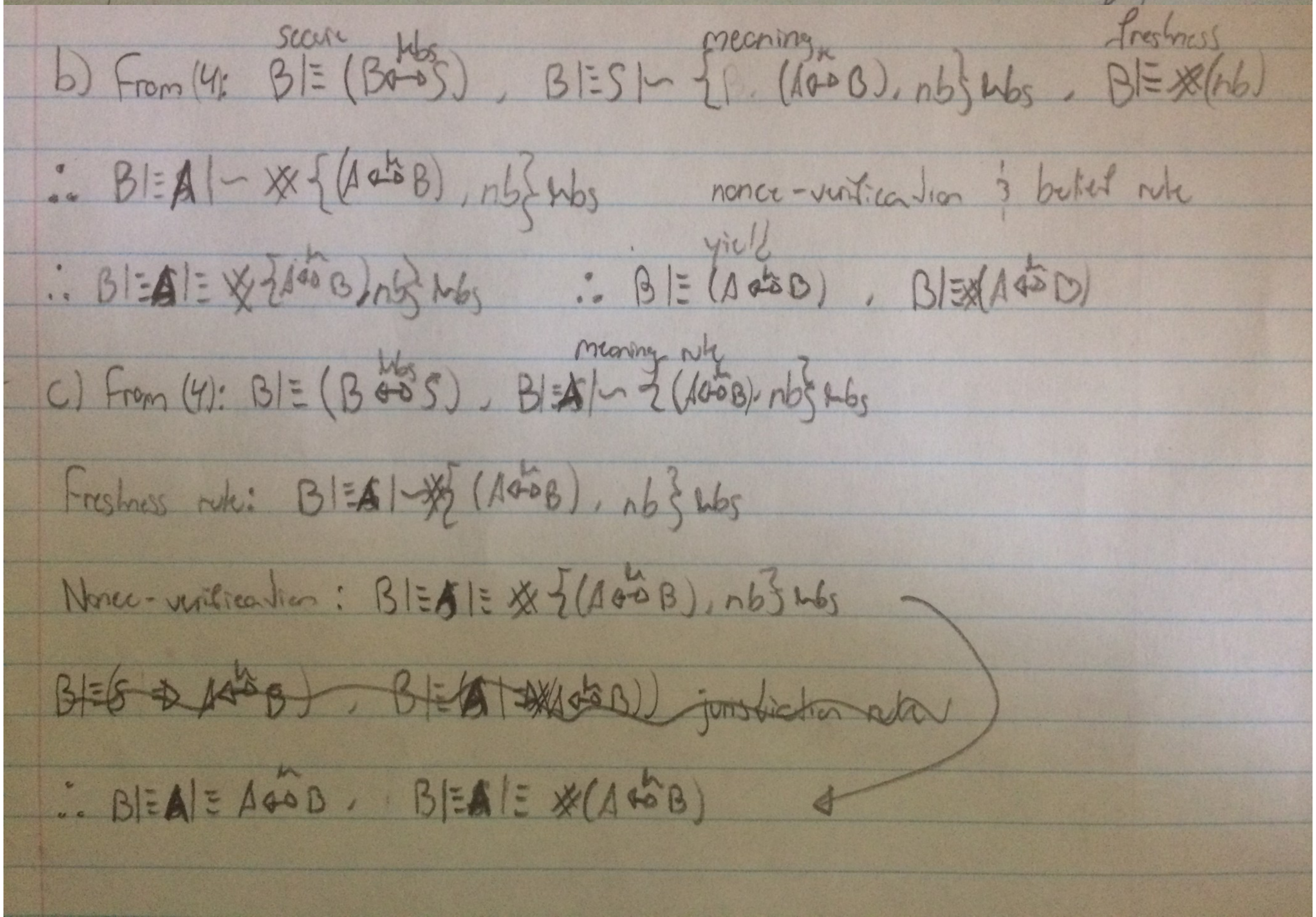
(4) $A \rightarrow B: \{(A \xleftrightarrow{K} B), nb\}_{K_{bs}}, \{nb\}_{K}$

a) From (3): $\overset{\text{secure}}{A |\equiv (A \xleftrightarrow{K_{as}} S)}$, $\overset{\text{meaning rule}}{A |\equiv S |\sim \{B, (A \xleftrightarrow{K} B), na\}_{K_{as}}}$, $\overset{\text{freshness rule}}{A |\equiv \#(na)}$

$\therefore A |\equiv S |\sim \#\{B, (A \xleftrightarrow{K} B), na\}_{K_{as}}$. Applying nonce verification & belief rule yields

a

$A |\equiv S |\equiv (A \xleftrightarrow{K} B)$ & $A |\equiv S |\equiv \#(A \xleftrightarrow{K} B)$



b) From (4): $\overset{\text{secure}}{B |\equiv (B \xleftrightarrow{K_{bs}} S)}$, $\overset{\text{meaning}}{B |\equiv S |\sim \{B, (A \xleftrightarrow{K} B), nb\}_{K_{bs}}}$, $\overset{\text{freshness}}{B |\equiv \#(nb)}$

$\therefore B |\equiv A |\sim \#\{(A \xleftrightarrow{K} B), nb\}_{K_{bs}}$ nonce-verification & belief rule yield

$\therefore B |\equiv A |\equiv \#\{(A \xleftrightarrow{K} B), nb\}_{K_{bs}}$ $\therefore B |\equiv (A \xleftrightarrow{K} B)$, $B |\equiv \#(A \xleftrightarrow{K} B)$

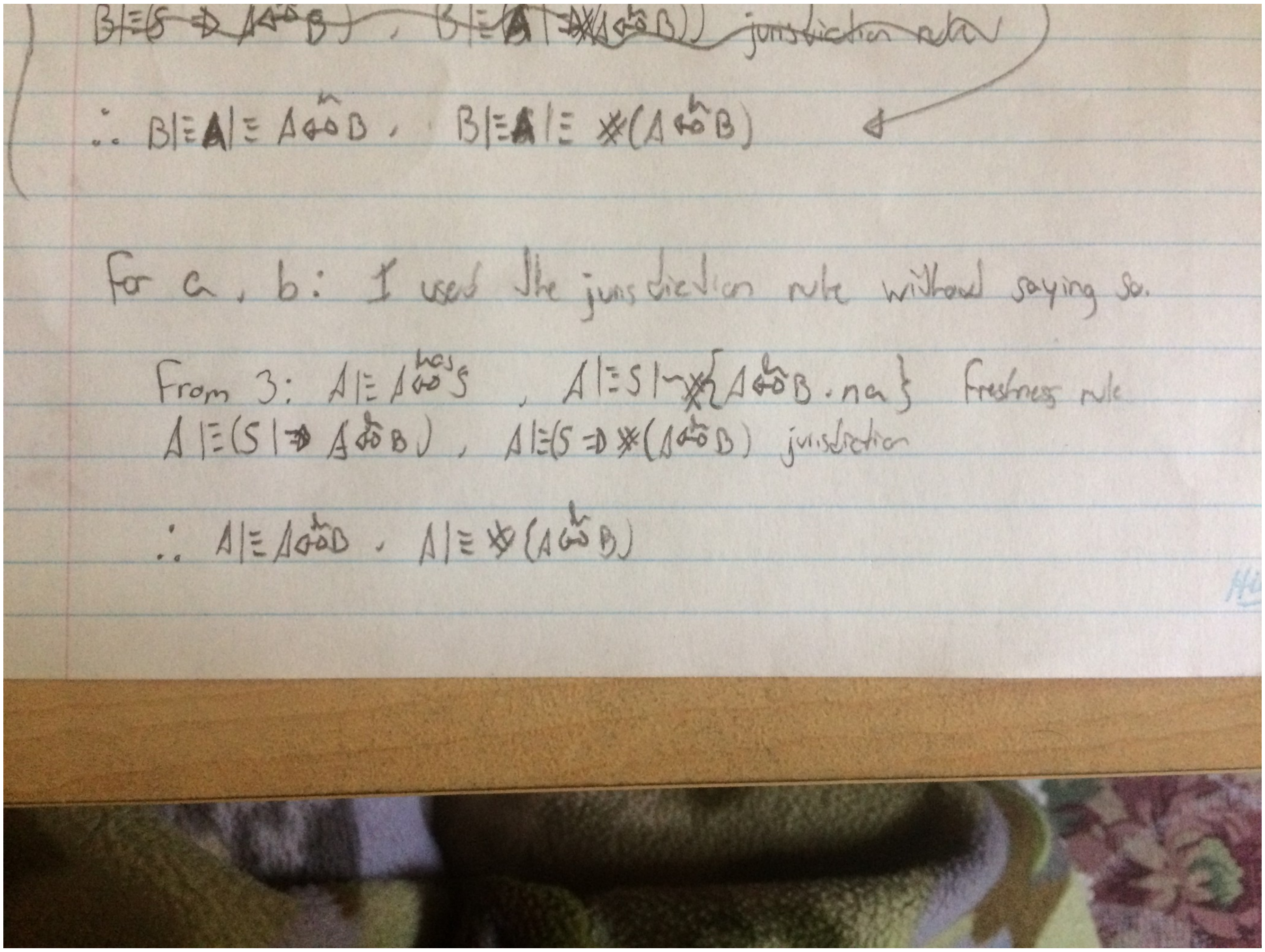
c) From (4): $B |\equiv (B \xleftrightarrow{K_{bs}} S)$, $\overset{\text{meaning rule}}{B |\equiv A |\sim \{(A \xleftrightarrow{K} B), nb\}_{K_{bs}}}$

Freshness rule: $B |\equiv A |\sim \#\{(A \xleftrightarrow{K} B), nb\}_{K_{bs}}$

Nonce-verification: $B |\equiv A |\equiv \#\{(A \xleftrightarrow{K} B), nb\}_{K_{bs}}$

~~$B |\equiv (S \Rightarrow A \xleftrightarrow{K} B)$, $B |\equiv (A |\Rightarrow \#(A \xleftrightarrow{K} B))$ jurisdiction rule~~

$\therefore B |\equiv A |\equiv A \xleftrightarrow{K} B$, $B |\equiv A |\equiv \#(A \xleftrightarrow{K} B)$



$B \mid\equiv (S \Rightarrow A \overset{k}{\leftrightarrow} B)$, $B \mid\equiv (A \mid \Rightarrow \#(A \overset{k}{\leftrightarrow} B))$ jurisdiction rule

$\therefore B \mid\equiv A \mid\equiv A \overset{k}{\leftrightarrow} B$, $B \mid\equiv A \mid\equiv \#(A \overset{k}{\leftrightarrow} B)$

For a, b: I used the jurisdiction rule without saying so.

From 3: $A \mid\equiv A \overset{has}{\leftrightarrow} S$, $A \mid\equiv S \mid\sim \#\{A \overset{k}{\leftrightarrow} B . na\}$ Freshness rule
$A \mid\equiv (S \mid\Rightarrow A \overset{k}{\leftrightarrow} B)$, $A \mid\equiv (S \Rightarrow \#(A \overset{k}{\leftrightarrow} B)$ jurisdiction

$\therefore A \mid\equiv A \overset{k}{\leftrightarrow} B$, $A \mid\equiv \#(A \overset{k}{\leftrightarrow} B)$