Advanced Security project:
→ VANET implementation

Bullet point list:

(1) Put in place a Key Exchange Protocol – with bilateral authentication

(2) Generate n keys from the exchanged key in step (1)

(3) Use keys generated in (2) to send informational messages that are encrypted using symmetric key encryption protocols

(4) Send message received notifications

(5) Put in place a protocol to resend messages that were not received, as well as stopping messaging an entity that hasn't responded to the last sent messages

Some specifications:

- One entity will exchange key with a second entity based on the physical distance they have between them
- This physical distance will be represented by a 2x2 grid, where an entity can move around and make random movements
- There won't be a third party that insures the authenticity of each entity at step (1)