Máme tu man in the middle attack. Základna A komunikuje se základnou B. Man in the middle dokáže číst všechny zprávy. Zároveň když posílá základna A zprávu do základny B, tak má man in the middle schopnost zprávu pozměňovat. Naším cílem je, aby man in the middle nedokázal úspěšně odposlechnout (a pochopit) o co ve zprávě jde, a také aby když zprávu pozmění, tak aby to základna B poznala.

1. A i B mají stejný seed na náhodnou generaci.
2. Oba náhodně vygenerují stejný klíč.
3. B zašifruje zprávu a pošle ji.
4. A ji rozšifruje klíčem a vygeneruje si další klíč s použitím seedu.
5. A podepíše zprávu a pošle ji B.
   1. Vytvoříme hash ze zprávy, který bude fungovat jako podpis
   2. Podpis se zašifruje pomocí vygenerovaného klíče
   3. Ke zprávě se přidá tento podpis
   4. Celková zpráva se zašifruje pomocí stejného klíče
6. B vygeneruje stejný klíč jako A a ověří podepsanou zprávu
   1. Celkovou zprávu dešifruje pomocí vygenerovaného klíče
   2. Oddělí zprávu od podpisu
   3. Ze zprávy vytvoří Hash
   4. Podpis dešifruje pomocí stejného klíče
   5. Porovná hash zprávy a podpisu, pokud jsou stejné, tak je zpráva ověřena
7. Opakujeme od kroku 1