Answers to Exercise 3:

3(a-i) Identify any vulnerability in this solution, and propose a solution to address any vulnerability that you have identified.

- **The PIN is decrypted in the ATM. The encrypted ID and PIN should be forwarded along with user's transaction request to Bank where the verification is performed.**

3(a-ii) Is there any other problem that you could identify from this application of symmetric cryptography?

- **The problem is the scale of the key management issue: (a) you use a different key for a different ATM, or (b) an identical key for all the ATMs. The implications for these options are obvious: (a) too many keys to generate, transport and manage; (b) if one key is compromised, then all communications will be at risk.**

3(b):
Use *DES(ECB)* and *DES(CBC)* modules in CrypTool, respectively, to encrypt the two messages, Msg1='*abcdefgh*', and Msg2='*abcdefghabcdefgh*'. The encryption key is: 11 22 33 44 55 66 77 88. Compare the four ciphertexts generated. What observation(s) can you make?

EBC mode:
(i)'*abcdefgh*' → 3F FC 1B 6B CF FC EE D5
(ii)'*abcdefghabcdefgh*' → 3F FC 1B 6B CF FC EE D5 3F FC 1B 6B CF FC EE D5

CBC mode:
(i)'*abcdefgh*' → 3F FC 1B 6B CF FC EE D5 2A 72 46 24 D4 3C 9D FC
(ii)'*abcdefghabcdefgh*' → 3F FC 1B 6B CF FC EE D5 87 77 BB C8 75 18 85 7B 5A 89 40 25 82 91 DD 78

Observations:
•In ECB mode, patterns in plaintext show up in ciphertext;
•In CBC mode, patterns in plaintext do not show up in ciphertext, and the ciphertext is one block longer than the plaintext, this is because the first ciphertext block is IV.

Topic 3 – quick question: