Secret key encryption (CS 915)

Post-Lab Assignment (100 marks)

Submit a report, addressing the following questions. There is no specific requirement for the format of the report, but we expect the report to be clear and concise.

- Task 1: 1) Briefly explain the results of this task with screenshots. 2) When you encrypt data using a password, you observe a warning “deprecated key derivation used”. Explain why you have such a warning. 3) Explain what is -pbkdf2 and why it is needed. [20]

- Task 2: 1) Briefly explain the results of this task with screenshots. 2) You encrypt pic_original.bmp in two methods: AES-128-CBC and AES-128-ECB. Use diagrams to explain how these two modes work. 3) Describe any difference in the output between the two methods and explain why. [20]

- Task 3: 1) Briefly explain the results of this task with screenshots. 2) You use "openssl enc -aes-128-cbc -e" to encrypt the three files using 128-bit AES with CBC mode. Describe the sizes of the encrypted files and explain why you have such sizes. 3) Describe what padding has been used in the encryption and explain how you verify that through the decryption process. [20]

- Task 4: 2) 1) Briefly explain the results of this task with screenshots. 2) Write down the substitution letters in the key (the top row being the plaintext letters) and explain how you have obtained them. [40]

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z