EHN 410 - Practical 2 Marksheet

Group Number:

Student Name	**Student Number**	**Signature**

Demo	**Mark**	**Total**
AES Functionality		
Subbytes		5
Shifting the rows		5
Mixing the Columns		5
X'OR the state with the expanded key		5
Creating the expanded key		5
AES Encryption		
Encrypt text (128-bit)		5
AES CBC		
Encrypt a file (128-bit)		5
Decrypt a file (128-bit)		5
192-, 256-bit keys		5
AES CFB		
Encrypt a file (128-bit)		5
Decrypt a file (128-bit)		5
192-, 256-bit keys		5
Doxygen		
ReadMe included (usage/compilation)		2
Class/function diagrams		2
Excerpts of code (only important aspects)		3
Meaningful comments/documentation		3
Total		**70**

Demo tests

Plain-text encryption

Text: "EHN 410 practical 2"

Password: "AES_encrypt"

Expanded key:

41	45	53	5f	65	6e	63	72	79	70	74	0	0	0	0	0
23	26	30	3c	46	48	53	4e	3f	38	27	4e	3f	38	27	4e
26	ea	1f	49	60	a2	4c	7	5f	9a	6b	49	60	a2	4c	7
18	c3	da	99	78	61	96	9e	27	fb	fd	d7	47	59	b1	d0
db	b	aa	39	a3	6a	3c	a7	84	91	c1	70	c3	c8	70	a0
23	5a	4a	17	80	30	76	b0	4	a1	b7	c0	c7	69	c7	60
fa	9c	9a	d1	7a	ac	ec	61	7e	d	5b	a1	b9	64	9c	c1
f9	42	e2	87	83	ee	e	e6	fd	e3	55	47	44	87	c9	86
6e	9f	a6	9c	ed	71	a8	7a	10	92	fd	3d	54	15	34	bb
2c	87	4c	bc	c1	f6	e4	c6	d1	64	19	fb	85	71	2d	40
b9	5f	45	2b	78	a9	a1	ed	a9	cd	b8	16	2c	bc	95	56

Encrypted message(Hex):

76 e6 4e f4 bc ec 28 12 6e 25 f8 40 2c a3 fb 26
3b 49 23 2a 49 11 2e 2c 81 71 e8 46 9b 9b 4 d8