Brandon Vo

Homework 1

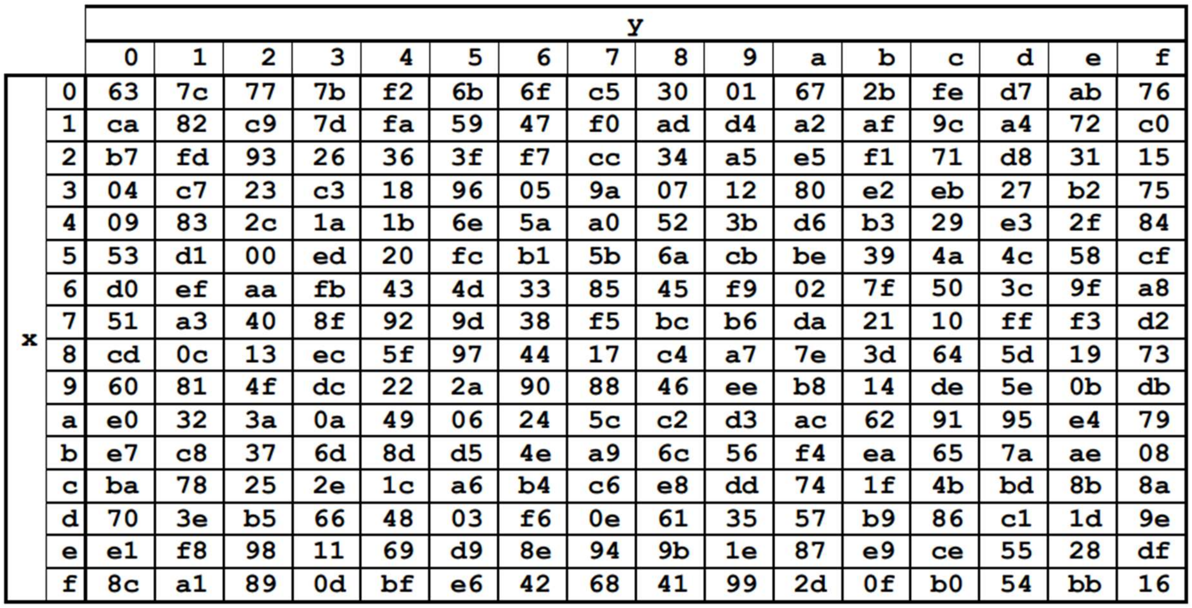
Advanced Encryption Standard (AES):

AES is a symmetric key encryption method designed as a successor to the Data Encryption Standard (DES) method of encryption where plaintext is put into an encryptor. Designed by the National Institute of Security Technology (NIST), it was intended to be used by the U.S. government and for public services as a versatile, widespread encryption method free for anyone to use. What makes AES different form other symmetric encryption algorithms is the use of block ciphers where data is partitioned into blocks and encoded in groups of bytes.

AES is one of the most widely used encryption method which comes in 3 types: 128-bit encryption, 192-bit encryption, 256-bit encryption. It works by treating data as blocks of bytes contained in a matrix and encoding the bytes in terms of their placement on the matrix. In addition to using block ciphers, AES utilizes the substitution and permutation methods to encrypt blocks of data.

The encryption method takes the initial cryptography key and initializes key expansion. The initial key is derived and used to a new set of encryption keys which will be used in the encryption of data[1].

1. SubBytes (Substitution): Places a byte of data into what is called the Rijndael substitution table. Within that substitution table, it will take the value of that byte and finds a new set of coordinates using XOR comparisons to find a replacement value based on the coordinates taken[2].



		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

The Rijndael substitution table

2. ShiftRows (Permutation)-In the matrix of bytes, the positions are all rotated left wise in a circular fashion, mixing the column arrangements.

[1] https://www.comparitech.com/blog/information-security/what-is-aes-encryption/

[2] https://formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng-html5.html

3. MixColumns (Substitution)-On the matrix, the blocks of data are multiplied with the pre-defined matrix table to create a new location for the blocks to be taken from[3].
4. AddRoundKey (Substitution)-This is the only step where the cipher key is used. The input we have from the previous steps combines an XOR comparisons with the cipher key to create a new set of values for the encoded message[4].

These 4 steps are repeated 9 times for each block. For each round where the 4 steps are repeated, the round key is used to generate another round key to be used for the next round of encryption. The decryption method is repeating the reverse of the steps above but using the inverse values in order to decrypt the message. The decryption method requires the cipher key used to encrypt the original message. Each step serves a purpose in obscuring the method of encryption in order to make reverse decryption without a cipher key much more difficult because the malicious third party would have to undo each encryption step multiple times, figuring out what round key was used for each round.

Pros:

- AES has no royalties and no exclusive design as it was released by the NIST, making AES a cost-effective method of encryption.
  - This makes AES the most widely used standard encryption mechanism for use by anyone[5].
- Implemented at the software and hardware level, making this encryption method extremely versatile.
  - The Rijndael block cipher was considered the most versatile method of encryption due to its ease of implementation[6].
  - Due to its simplicity, AES is faster than most symmetric encryption algorithms and asymmetric encryption algorithms
  - Demands very little hardware power, requiring very little CPU power and RAM
- Uses atleast 128-bit encryption as opposed to its predecessor, DES's, 64-bit and 56-bit encryption
  - The 128-bit encryption alone would require a brute force attack of 2^{128} attempts to break through, making brute-force methods using our current technology highly impractical.
  - Has no record of being cracked and is expected to resist attacks by the higher processing power of quantum computing as well[7].
- There are no restrictions on the keys that can be generated because there are no keys that would be considered easy to break[8].
- Enforces large key sizes of 128-bit, 192-bit, or 256-bit to make brute force attacks much more difficult.

Cons:

- The weak spot with AES, along with all symmetric cryptography measures, is the encryption key itself. Access to the encryption key is enough to decode the information and leave important data vulnerable.

[3] https://www.trentonsystems.com/blog/aes-encryption-your-faqs-answered
[4] https://www.youtube.com/watch?v=O4xNJsjtN6E
[5] https://vivadifferences.com/difference-between-aes-and-des-algorithms-in-network-security/
[6] https://www.comparitech.com/blog/information-security/what-is-aes-encryption/
[7] Rao, Sandeep & Mahto, Dindayal & YADAV, DILIP & Khan, Danish. (2017). The AES-256 Cryptosystem Resists Quantum Attacks. International Journal of Advanced Research in Computer Science. 8. 404-408.
[8] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf, page 26

- As mentioned above, the method of encryption is the same for all blocks of data. Every byte of data is encrypted using the same 4 steps above, making reverse engineering a possible threat.[9]
- The cipher key plays only a small role in encoding the message. It's used only in one step compared out of the 4 steps.
    - This leads to an issue called a side-channel attack where a malicious 3rd party will pick up on the data being encoded and use that to reverse engineer the encoding procedure[10].
- The encoding mechanism is deterministic. The same input with the same key will produce the same output every time. This leaves the encryption algorithm vulnerable to brute force attacks[11].
- Because AES uses a block cipher for encryption, it requires managing data in groups of 16-bytes, so it will pad out any non-equal data to fit a full-sized block.
    - This can lead to AES increasing the size of data considerably[12].
- The encryption mechanism is extremely simple which makes reverse engineering a very likely concern.

[9] https://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-AES.html
[10] https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
[11] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf, page 26
[12] https://proprivacy.com/guides/aes-encryption