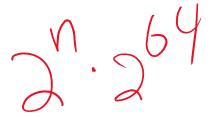
# Crypto VIII: Theory of Block Ciphers *ECE 4156/6156 Hardware-Oriented Security and Trust*

Spring 2024
Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

### Reading Assignment

• Please read Chapter 6 of the course textbook by Katz and Lindell

#### Confusion



- Hide the relationship between the plaintext, ciphertext and key
  - Consider an extreme case: a key dependent lookup table mapping 64 bits of plaintext to 64 bits of ciphertext
    - This would provide sufficient security
    - Problem: if the key has *n* bits, need  $(2^n)^*(2^{64}) = 2^{(n+64)}$  amount of memory
      - Note that  $2^{40}$  = Terabyte (TB), and a single storage rack in a server farm can handle a few TB
  - Modern block ciphers use much smaller tables (so-called "substitution boxes" or s-boxes)
    - Smaller size may allow brute-force attacks to succeed
    - In other words, the reduction in size helps make the block cipher computable with reduced memory but also helps the adversary

	Ī	У															
		0	1	2	3	4	5	6	7	8	9	a	b	C	d	е	f
x	0	63	7c	77	7b	£2	6b	6£	с5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	<b>c</b> 9	7d	fa	59	47	£0	ad	d4	a2	af	9c	a4	72	<b>c</b> 0
	2	b7	fd	93	26	36	3£	£7	O C	34	a5	e5	f1	71	q8	31	15
	3	04	<b>c</b> 7	23	с3	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	£9	02	7£	50	3c	9£	a8
	7	51	a3	40	8£	92	9d	38	£5	bc	b6	da	21	10	ff	£3	d2
	8	cd	0c	13	ec	5£	97	44	17	<b>c4</b>	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	ďb
	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	£4	ea	65	7a	ae	08
	С	ba	78	25	2e	1c	a6	b4	<b>c</b> 6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	<b>b</b> 5	66	48	03	£6	0e	61	35	57	b9	86	c1	1d	9e
	е	e1	£8	98	11	69	d9	8e	94	9b	1e	87	e9	се	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 7. S-box: substitution values for the byte xy (in hexadecimal format).

#### Diffusion

• Spread the influence of changing a few bits of plaintext or the key over as much of the ciphertext as possible

• Helps hide statistical relationships

#### Diffusion

- Spread the influence of changing a few bits of plaintext or the key over as much of the ciphertext as possible
  - Helps hide statistical relationships

### Combining Confusion and Diffusion

- Substitute (confuse) and permute (diffuse)
  - Product cipher
  - Substitution-permutation (SP) network
- Consider AES
  - Diffusion: ShiftRows and MixColumns
    - Both are linear
  - Confusion: SubBytes (also referred to as S-Boxes)
    - Nonlinear
  - All operations are fairly simple (fast) to compute
- Iterated block cipher
  - Two rounds of AES is not strong
  - AES has between 10 and 14 rounds (depending on chosen key size)

## Feistel Networks (not used by AES)



- Horst Feistel worked for IBM Research
- Take a block of length n and divide into two equal halves L and R
  - *n* must be even
- Define an iterated block cipher
- This function is reversible
- Therefore, a cipher based on a Feistel network is guaranteed to be invertible
- Note that reversibility is not dependent on f being reversible
- Further note that the same algorithm works for decryption

• 
$$L_i = R_{i-1}$$

- $R_i = L_{i-1} \text{ XOR } f(R_{i-1}, K_i)$ 
  - where  $K_i$  is the subkey used in round i and f is the round function used

• 
$$L_{i-1}$$
 XOR  $f(R_{i-1}, K_i)$  XOR  $f(R_{i-1}, K_i) = L_{i-1}$ 



### SubBytes/S-Box Design

- S-Box: a mapping from m bits to n
- Typically implemented as a look-up table
- Non-linear and non-degenerate, i.e., no way to compute the relation with a function
  - => must perform a look-up in memory!
- Boolean properties: balance of zeros and ones, no correlations between different bit combinations, avalanche effect
  - Avalanche: one bit of input should on average change approximately half of the output bits
- Provides strong resistance to cryptanalysis
  - In other words, forces the adversary to only use brute force attacks