Information Security 2022
2nd Project

Prof. Junbeom Hur

TA. Woonghee Lee
(whlee@isslab.korea.ac.kr)

Information System Security Lab.,
Department of Computer Science and Engineering,
Korea University, Seoul, Korea

Finding a Hash Collision pair

- Given a hash function H(m, t), find a message pair which has the same hash value, but different messages when t = 5.
- H(m, t)
  - m: message
  - t: special value for a hash function
  - Input m is a 256-bit message, m = (m[0], m[1], …, m[31])
  - Output o is a 128-bit value, o = (o[0], o[1], …, o[15])
  - Each of o[i] and m[i] is a unit vector of which size is 8-bit

Hash Function, H(m, t)

H(m, t)

```
1. $A_0$= (m[0], m[1], …, m[15])
2. $B_0$= (m[16], m[17], …, m[31])
3. For $i$ = 0, 1, …, $t-2$ :
4.         $rb_i = (B_i[0], B_i[1], B_i[2], B_i[3])$
5.         $A_{i+1} = Round(rb_i, A_i)$
6.         $B_{i+1} = Round((\mathrm{i}, \mathrm{i}+1, \mathrm{i}+2, \mathrm{i}+3), A_i)$
7. End For
8. $rb_{t-1} = (B_{t-1}[0], B_{t-1}[1], B_{t-1}[2], B_{t-1}[3])$
9. $A_t$= $Round'(rb_{t-1}, A_{t-1})$
10. $O = A_t \bigoplus A_0 \bigoplus B_0$
    (which is $A_t[0] \bigoplus A_0[0] \bigoplus B_0[0], \dots, A_t[15] \bigoplus A_0[15] \bigoplus B_0[15]$)
```

Round and Round′ Function

$\boldsymbol{Y = Round(rb, X)}$

Each of rb and X is a 32-bit value which can be represented by rb = (rb[0], rb[1], rb[2], rb[3]) and X = (X[0], X[1], … , X[15]).

Each of rb[i] and X[i] is a unit vector of which size is 8-bit.

1. $(Y[0], \dots, Y[3]) = F\big(rb, (X[0], \dots, X[3])\big) \oplus (X[4], \dots, X[7])$
2. $(Y[4], \dots, Y[7]) = (X[8], \dots, X[11])$
3. $(Y[8], \dots, Y[11]) = (X[12], \dots, X[15])$
4. $(Y[12], \dots, Y[15]) = (X[0], \dots, X[3])$

$\boldsymbol{Y = Round'(rb, X)}$

1. $(Y[0], \dots, Y[3]) = (X[4], \dots, X[7])$
2. $(Y[4], \dots, Y[7]) = F\big(rb, (X[0], \dots, X[3])\big) \oplus (X[8], \dots, X[11])$
3. $(Y[8], \dots, Y[11]) = (X[12], \dots, X[15])$
4. $(Y[12], \dots, Y[15]) = (X[0], \dots, X[3])$

(F function will be described at slide #5)

F Function

$\boldsymbol{Y = F(rb, X)}$

Each of rb and X is a 32-bit value which can be represented by rb = (rb[0], rb[1], rb[2], rb[3]) and X = (X[0], X[1], X[2], X[3]).

Each of rb[i] and X[i] is a unit vector of which size is 8 bit.

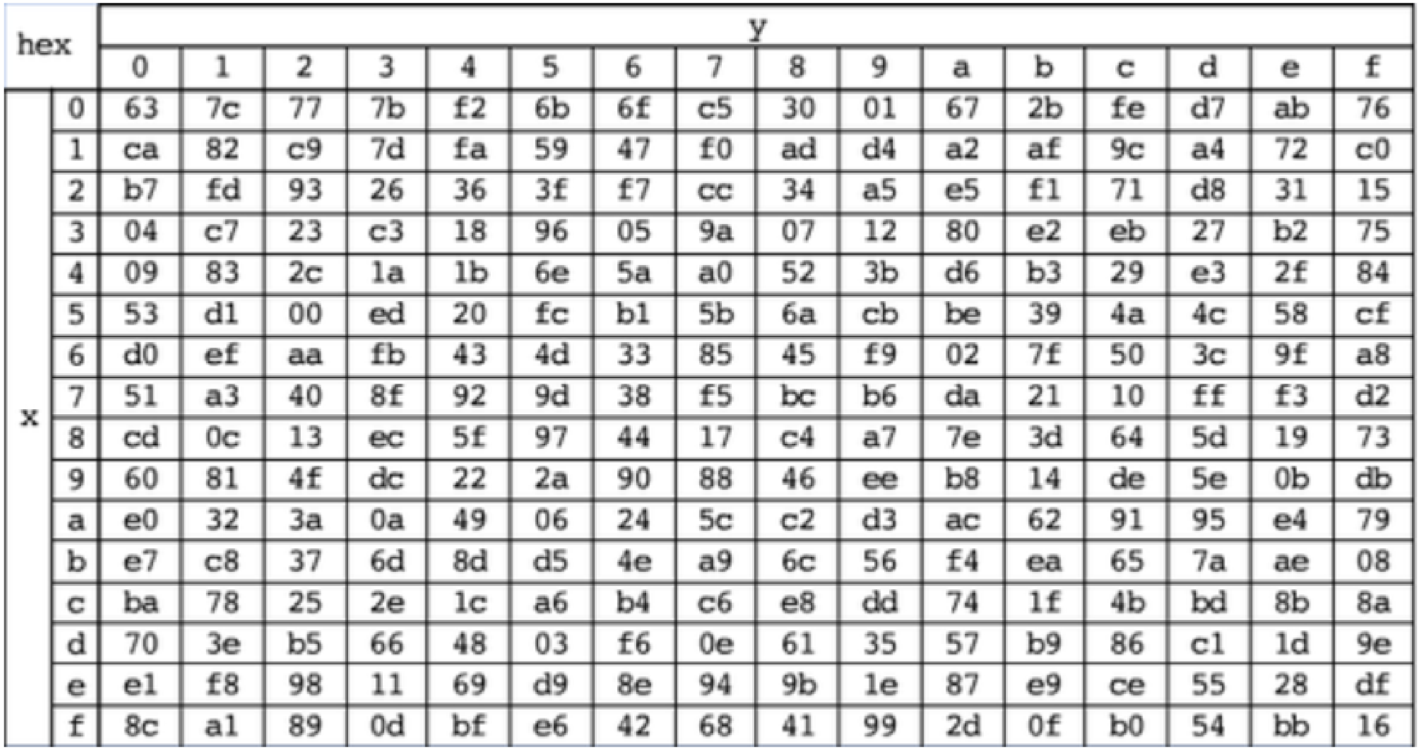
1. $p[i] = X[i] \oplus rk[i] \quad (for\ i = 0,1,2,3)$
2. $q[i] = S(p[i]) \quad (for\ i = 0,1,2,3)$ // AES S-box function
3. $y^T = M \cdot q^T$ // AES MixColumn function

✓ $S(p)$ is the same as S-box of AES

✓ $y^T = M \cdot q^T$ is the same as AES MixColumn function

S-box Function

- S-box function: $\boldsymbol{S}(\boldsymbol{xy})$
  - Input is an 8-bit value represented by hexadecimal number
  - ex) If xy = d2, S(d2)=b5 given the S-box table



hex		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

$y^T = M \cdot x^T$ - 32bit Matrix Product

$\boldsymbol{y^T = M \cdot x^T}$

- Same as the AES MixColumn
- The 32-bit value x is composed of four 8-bit unit vectors (a 1×4 matrix with size 4): x = (x[0],x[1],x[2],x[3])
- The multiplication operations are conducted in GF(2^8)

$$y^T = \begin{bmatrix} y[0] \\ y[1] \\ y[2] \\ y[3] \end{bmatrix} = M \cdot x^T = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} x[0] \\ x[1] \\ x[2] \\ x[3] \end{bmatrix}$$

Submission Guideline

- **Please upload the followings as a single compressed file into Blackboard**

1. Source codes and exe files for solution **(C and C++ are encouraged, but if you want you can use Python, Java, etc).**
   - You may use C++ to implement those functions easily.
2. A message pair and a hash value (.txt)
3. Report **(.doc, .hwp, or pdf file)**
   - It must include detailed analysis of Hash function and description of your solution. Even if your final answer is right, your score would be deducted if such description is not enough.
4. Deadline: **2022. Dec. 4, 23:59**

❖ **Late submission, or any kind of plagiarism will result in 0 point**