



Cryptography

Exercises

Enero 31, 2023

1. Modular Arithmetic

Please do the following exercises without a calculator. Solve them and if you have questions please ask for help

1. For each of the following exercises, give the result as an integer greater or equal than 0 and less than the module. For example $-3501 \bmod 7 = 6$.

- a) $-81 \bmod 90$
- b) $-162 \bmod 81$
- c) $-100 \bmod 24$
- d) $-5303 \bmod 63$
- e) $-3 \bmod 1111$

2. In the following exercises construct a multiplication table as we did it in class. Then see which elements have a multiplicative inverse. For example in \mathbb{Z}_9 , 5 has multiplicative inverse:2, since $5 * 2 \bmod 9 = 1$.

- a) \mathbb{Z}_7 ,
- b) \mathbb{Z}_7^*
- c) \mathbb{Z}_8
- d) \mathbb{Z}_{17}
- e) \mathbb{Z}_{10}
- f) \mathbb{Z}_{10}^*
- g) \mathbb{Z}_{20}
- h) \mathbb{Z}_{20}^*

In general can you say when an element in \mathbb{Z}_n has an inverse?

3. Using the extended Euclidean algorithm, find the integer x such that $5 * x \bmod 13 = 1$
4. Using the extended Euclidean algorithm, find the integer x such that $5 * x \bmod 7 = 1$
5. Find a way to convince yourself that $-a \bmod m = m - (a \bmod m)$

```

Extended_Euclides( $a, b$ )
1.    $u \leftarrow a; v \leftarrow b$ 
2.    $x_1 \leftarrow 1, y_1 \leftarrow 0, x_2 \leftarrow 0, y_2 \leftarrow 1;$ 
3.   while  $u \neq 0$  do
3.1.    $q \leftarrow \lfloor v/u \rfloor, r \leftarrow v - qu, x \leftarrow x_2 - qx_1, y \leftarrow y_2 - qy_1;$ 
3.2.    $v \leftarrow u, u \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x, y_2 \leftarrow y_1, y_1 \leftarrow y;$ 
4.    $d \leftarrow v, x \leftarrow x_2, y \leftarrow y_2$ 
5.   return  $(d, x, y)$ 

```

6. The following algorithm receives as input two integers a and b , and as output gives the d , the greatest common divisor; and x and y such that $d = ax + by$. Prove this algorithm with the pair $(5, 26)$, what are the values of the output (d, x, y) . Register the values of the variables $u, v, q, r, x_1, y_1, x_2, y_2, x, y$.
7. Use the previous algorithm to find valid keys $K = (a, b)$, where $\gcd(a, n) = 1$ and $a^{-1} \bmod n$ for the affine cipher for each of the following sizes of alphabet
 - a) $n = 21$
 - b) $n = 19$
 - c) $n = 30$
8. The function $\phi(n)$ is called the Euler phi function and denotes the number of integers between 1 and n for $n \geq 1$ which are relatively prime to n . We can calculate $\phi(n)$ using the following properties:
 - If p is a prime number, then $\phi(p) = p - 1$
 - If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m) \cdot \phi(n)$
 - If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime factorization of n , then

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$$

Using the previous definition calculate :

- a) $\phi(11)$
 - b) $\phi(101)$
 - c) $\phi(22)$
 - d) $\phi(21)$
 - e) $\phi(30)$
 - f) $\phi(42)$
9. If the size of the alphabet is 30, how many different keys are available for affine cipher. Tip: the Euler's function can help you to find this number.
 10. If the size of the alphabet is 19, how many different keys are available for affine cipher. Tip: the Euler's function can help you to find this number.
 11. If the size of the alphabet is 21, how many different keys are available for affine cipher. Tip: the Euler's function can help you to find this number.

12. The following algorithm generates the subkeys for each round of AES, given a key of 128 bits. It incorporates the following operations: $\text{ROTWORD}(B_0, B_1, B_2, B_3)$ performs a cyclic shift of the four bytes B_0, B_1, B_2, B_3 , i.e.

$$\text{ROTWORD}(B_0, B_1, B_2, B_3) = B_1, B_2, B_3, B_0,$$

$\text{SUBWORD}(B_0, B_1, B_2, B_3)$ applies S-box to each of the four bytes B_0, B_1, B_2, B_3 , i.e.

$$\text{SUBWORD}(B_0, B_1, B_2, B_3) = B'_0, B'_1, B'_2, B'_3$$

$Rcon$ is an array of 10 words. These are constants that are defined in hexadecimal notation

Algorithm 3.6: KEYEXPANSION(key)

external ROTWORD, SUBWORD

$RCon[1] \leftarrow 01000000$

$RCon[2] \leftarrow 02000000$

$RCon[3] \leftarrow 04000000$

$RCon[4] \leftarrow 08000000$

$RCon[5] \leftarrow 10000000$

$RCon[6] \leftarrow 20000000$

$RCon[7] \leftarrow 40000000$

$RCon[8] \leftarrow 80000000$

$RCon[9] \leftarrow 1B000000$

$RCon[10] \leftarrow 36000000$

for $i \leftarrow 0$ **to** 3

do $w[i] \leftarrow (key[4i], key[4i + 1], key[4i + 2], key[4i + 3])$

for $i \leftarrow 4$ **to** 43

$\left\{ \begin{array}{l} temp \leftarrow w[i - 1] \\ \text{if } i \equiv 0 \pmod{4} \end{array} \right.$

do $\left\{ \begin{array}{l} \text{then } temp \leftarrow \text{SUBWORD}(\text{ROTWORD}(temp)) \oplus RCon[i/4] \\ w[i] \leftarrow w[i - 4] \oplus temp \end{array} \right.$

return $(w[0], \dots, w[43])$

Using Algorithm 3.6 (shown above), generate the subkey for the first round if the key in hexadecimal notation is $A0A0A0A0\ F0F0F0F0\ 0F0F0F0F\ 0A0A0A0A$.

13. Given a block of plaintext of only 0's calculate the result of the first round to encipher using AES. Use the key and the subkey from the previous point.

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