1. Consider a symmetric encryption scheme with encryption function $E(k, m) = 3m + k \mod 8$. for plaintext $m \in \mathbb{Z}_8$ and key $k \in \mathbb{Z}_8$. Suppose every key $k \in \mathcal{K}$ is chosen with equal probability.

   (a) What is the decryption function? (10%)

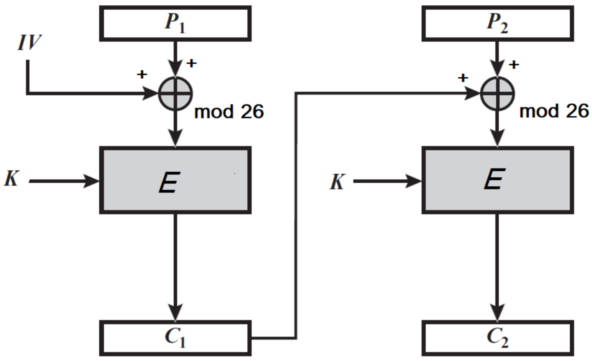
   (b) Given any plaintext m and its ciphertext c, derive an attack on the encryption system. (10%)

2. Euler's theorem says that $a^{\phi(n)} \equiv 1 \pmod{n}$ for $\gcd(a, n) = 1$, where $\phi(n) = \prod_{i=1}^{t} p_i^{a_i - 1}(p_i - 1)$ for $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$. Consider the number 13^{1002}. What are the last two digits of 13^{1002} in decimal form? Explain how you get the answer. (15%)

3. Find a *monic* polynomial that is a greatest common divisor of both $(x^4 + 8x^3 + 7x + 8)$ and $(2x^3 + 9x^2 + 10x + 1)$ over $GF(11)$. (15%)

4. Determine the multiplicative inverse of $\{03\}$ (in hexadecimal) in $GF(2^8) = \mathbb{Z}_2[x]/\langle x^8 + x^4 + x^3 + x + 1\rangle$. (15%)

5. A ciphertext *hgaa* is encrypted using the Hill cipher in the cipher block chaining mode as in the following figure, where $P_1, P_2 \in \mathbb{Z}_{26}^2$, $IV = (12\ 5) \in \mathbb{Z}_{26}^2$, the addition is modulo 26, and the key is $K = \begin{bmatrix} 7 & 3 \\ 2 & 5 \end{bmatrix}$. (Recall that the Hill cipher has an encryption algorithm $E(K, P) = PK \mod 26$ for $P \in \mathbb{Z}_{26}^2$ and a plaintext will be transformed to a string of numbers over $\mathbb{Z}_{26}$ before encryption.)



   (a) What is the decryption function? Plot it. (10%)

   (b) What are P_1, P_2 and the original plaintext? (10%)

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

(See the next page for more problems.)

6. Consider the following key expansion algorithm that generates 3 words of roundkeys from input a 4-byte key:

```
KeyExpansion (byte key[4])
{
 word w[3];
 w[0]=( key[0], key[1], key[2], key[3]);
   w[1]= g(w[0]);
   w[2]= w[1]+g(w[1]);

 return w;
}
```

where the addition is in $GF(2^8)$ and g takes an input of four bytes and outputs four bytes as follows:

```
g(byte key[4])= (Sbox(key[1]), Sbox(key[2]), Sbox(key[3]), Sbox(key[0])).
```

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
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 S-box is given as above. (Ex, $Sbox(\{95\}) = \{2A\}$.)
What is the output of KeyExpansion({01},{02},{03},{04}) in hexadecimal? (20%)