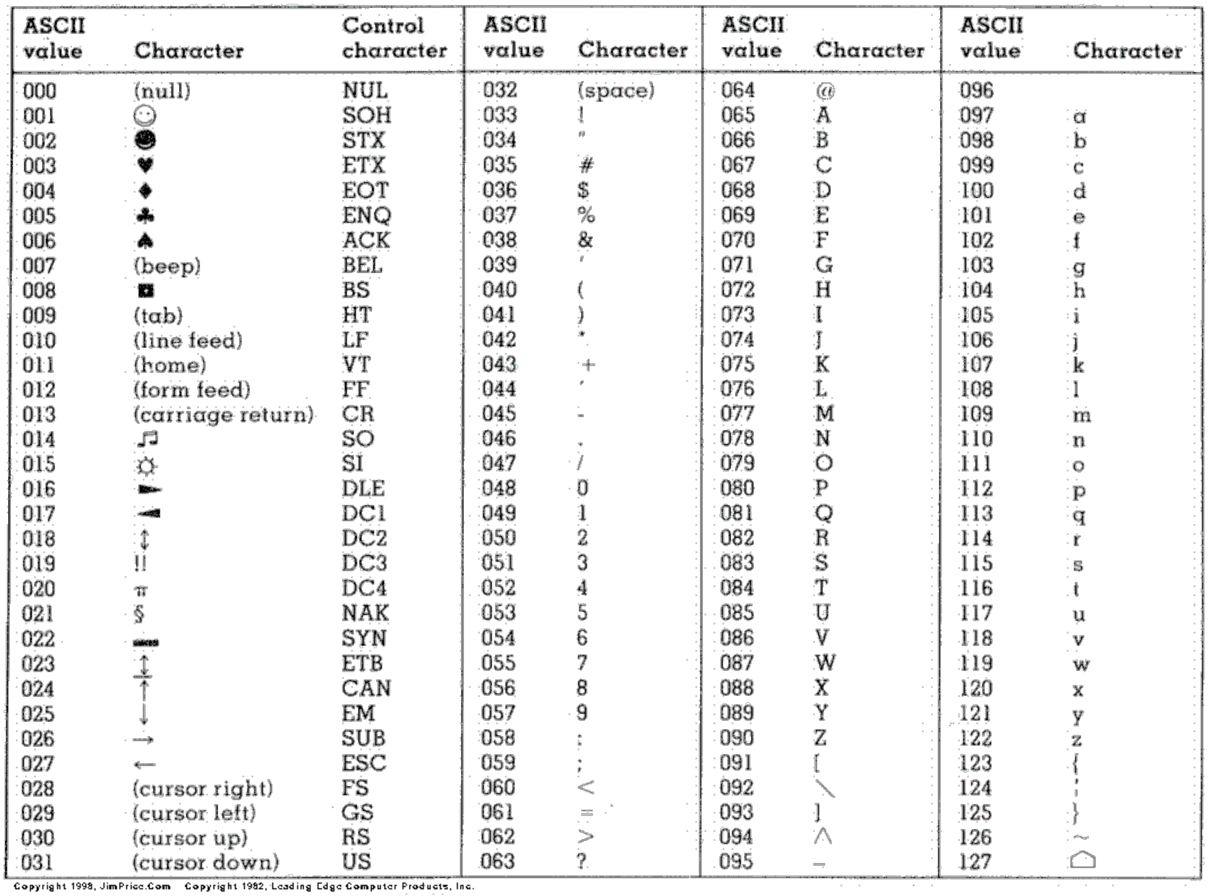
CIS 475 - INTRODUCTION TO CRYPTOGRAPHY
EXAM 2 – Spring 2019
75 minutes

Name:

1. In the ELGAMAL public key crypto system with P =227, Bob uses the smallest odd generator g for Z_p*, and the secret exponent a = 8. Compute the values of g and the public half mask H. One morning Bob receives a ciphertext from Alice containing the sequence (85,53), where the half mask is the first element and cipher is the second. What is the ASCII character that Alice sent to Bob? Show all your work including the modular inverse computation.



ASCII value	Character	Control character	ASCII value	Character	ASCII value	Character	ASCII value	Character
000	(null)	NUL	032	(space)	064	@	096	
001	☺	SOH	033	!	065	A	097	a
002	☻	STX	034	"	066	B	098	b
003	♥	ETX	035	#	067	C	099	c
004	♦	EOT	036	$	068	D	100	d
005	♣	ENQ	037	%	069	E	101	e
006	♠	ACK	038	&	070	F	102	f
007	(beep)	BEL	039	'	071	G	103	g
008	◘	BS	040	(	072	H	104	h
009	(tab)	HT	041	)	073	I	105	i
010	(line feed)	LF	042	*	074	J	106	j
011	(home)	VT	043	+	075	K	107	k
012	(form feed)	FF	044	'	076	L	108	l
013	(carriage return)	CR	045	-	077	M	109	m
014	♫	SO	046	.	078	N	110	n
015	☼	SI	047	/	079	O	111	o
016	►	DLE	048	0	080	P	112	p
017	◄	DC1	049	1	081	Q	113	q
018	↕	DC2	050	2	082	R	114	r
019	!!	DC3	051	3	083	S	115	s
020	π	DC4	052	4	084	T	116	t
021	§	NAK	053	5	085	U	117	u
022	▬	SYN	054	6	086	V	118	v
023	↨	ETB	055	7	087	W	119	w
024	↑	CAN	056	8	088	X	120	x
025	↓	EM	057	9	089	Y	121	y
026	→	SUB	058	:	090	Z	122	z
027	←	ESC	059	;	091	[	123	{
028	(cursor right)	FS	060	<	092	\	124	¦
029	(cursor left)	GS	061	=	093	]	125	}
030	(cursor up)	RS	062	>	094	^	126	~
031	(cursor down)	US	063	?	095	_	127	⌂

2. In the ELGAMAL ELLIPTIC CURVE crypto system, Bob uses the curve $y^2 = x^3+3x-1$ modulo $q = 23$. As his generator Bob uses the point $G = (2,6)$ and as the secret multiplier he used the constant $N = 4$. This determines Bob's half mask $H_B = 4*G = (14,5)$. Bob then published his public keys (q, a , b , G, H_B). One evening Bob receives from Alice the pair of points $C = (5,1)$ and $H_A = (21,13)$, where C is the cipher and H is the half mask.

    a. Show how Bob recovers the full mask F from the half mask H_A. What is the value of F?
    b. Show how Bob recovers the plaintext M form C and F. What is the value of M?