Introduction to Cryptography Final Fall 2019

Name:_____ Score: /50

1. [5 pts] Data compression is often used in data storage and transmission. Suppose you want to use data compression in conjunction with encryption. Does it make more sense to:

    a) The order does not matter -- either one is fine.

    b) Compress then encrypt.

    c) The order does not matter -- neither one will compress the data.

    d) Encrypt then compress.

2. [5 pts] Consider the following five events:

    1) Correctly guessing a random 128-bit AES key on the first try.
    2) Winning a lottery with 1 million contestants (the probability is $1/10^6$)
    3) Winning a lottery with 1 million contestants 5 times in a row (the probability is $(1/10^6)^5$)
    4) Winning a lottery with 1 million contestants 6 times in a row.
    5) Winning a lottery with 1 million contestants 7 times in a row.

What is the order of these events from most likely to least likely?

2, 3, 4, 1, 5

2, 3, 5, 4, 1

2, 3, 4, 5, 1

3, 2, 5, 4, 1

3. [5 pts] Suppose that using commodity hardware it is possible to build a computer for about $200 that can brute force about 1 billion AES keys per second. Suppose you wants to run an exhaustive search for a single 128-bit AES key and was willing to spend 4 trillion dollars to buy these machines. How long would you take to brute force this single 128-bit AES key with these machines? Ignore additional costs such as power and maintenance.

    a. More than a 100 years but less than a million years
    b. More than a month but less than a year
    c. More than a day but less than a week
    d. More than a million years but less than a billion (10^9) years
    e. More than a billion (10^9) years

4. [5 pts] Let M = C = K = {0,1,2,…,255} and consider the following cipher defined over (K,M,C):

    $E(k,m) = m+k \pmod{256}$

    $D(k,c) = c-k \pmod{256}$

    Does this cipher have perfect secrecy?

    a) Yes.
    b) No, only the One Time Pad has perfect secrecy.
    c) No, there is a simple attack on this cipher.

5. [10 pts] Why are hash functions used and what are their properties?

6. [20 pts] In a t*hree- prime* RIVEST-SHAMIR-ADLEMAN (RSA) public- key cryptosystem, with n = 1771, e = 7 and 1 bit salting, Bob receives a ciphertext from Alice that is *274 mod 1771*. Compute the secret exponent *d* and Alice's plaintext using Chinese Remainder Theorem. Circle in the ASCII table the plaintext character that Alice sent to Bob.

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	¶	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	⌂