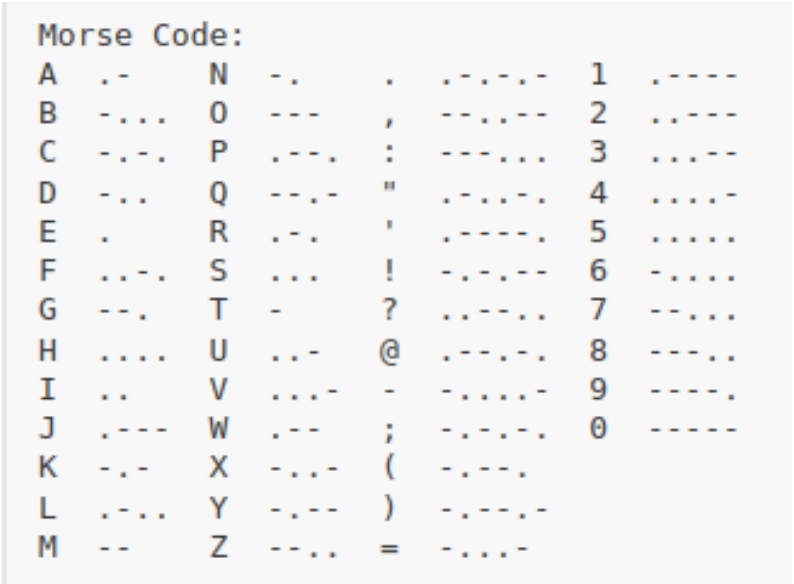
Cryptography (BITS F463) Midsem Exam (2023)

There are 3 questions in all and total marks are $10+(2+3+5)+(5+5) = 30$. Please show all steps in proofs or computations (using efficient algorithms). Calculators are allowed. This is a **closed book exam**. Time: 90 minutes.

1. Mr. James Bond was presented with an intercept:
   `KCJAA IJNLD ERLRA YDEFA HTOER LLKSI`
   `10 001 101 0 000`

   Along with the above short ciphertext the intelligence agencies also provided the following background information on it:
   • It is confirmed that the sender and the receiver have neither met each other nor communicated by other means for a long time. Thus it is very unlikely that they have a shared key with them which they are using for communication.
   • Both the sender and the receiver have immense knowledge about old communication / encryption technologies. Sleuths confirm that among other things the sender was recently consulting books on Morse codes in the local library.

   Help Mr. Bond cryptanalyze the intercept.



Morse Code:							
A	.-	N	-.	.	.-.-.-	1	.----
B	-...	O	---	,	--..--	2	..---
C	-.-.	P	.--.	:	---...	3	...--
D	-..	Q	--.-	"	.-..-.	4	....-
E	.	R	.-.	'	.----.	5	.....
F	..-.	S	...	!	-.-.--	6	-....
G	--.	T	-	?	..--..	7	--...
H	....	U	..-	@	.--.-.	8	---..
I	..	V	...-	-	-....-	9	----.
J	.---	W	.--	;	-.-.-.	0	-----
K	-.-	X	-..-	(	-.--.		
L	.-..	Y	-.--	)	-.--.-		
M	--	Z	--..	=	-...-		

2. Using the notation used in the AES algorithm, and the GF(2^8) used in the AES algorithm ($\mathbb{Z}_2[x]/\left(x^8 + x^4 + x^3 + x + 1\right)$), compute the following:
   (a) $\{DC\} \oplus \{DA\}$.
   (b) $\{CD\} \bullet \{BC\}$.
   (c) $\{AB\}^{-1}$.

3. The RSA cryptosystem is insecure when its public key (e, n) has $e = 3$.
   (a) Design a polynomial-time algorithm to recover the plaintext m, when you are given the ciphertexts $c_1 = \text{RSA}_{(3,n)}(m)$ and $c_2 = \text{RSA}_{(3,n)}(m+1)$.
   (b) Using the above polynomial-time algorithm, find m if $c_1 = 3728$, $c_2 = 5078$, and $n = 8633$.