Problem 2. Alphabet Soup [12 points]

For each name or acronym, write the letter of all terms that apply. Be aware that nonsense names and terms may have been added.

Name	Terms that Apply
RSA	
RZA	
OAEP	
DES	
CTR	
ElGamal	
CPA	
AES	
ODB	
CBC	
PGP	
CCA	
SHA-1	
3DES	
2PAC	
RC5	
MD5	

Letter	Term
A	Cipher Block Mode.
B	Supports Public-Key Encryption.
C	Supports Digital Signatures.
D	Block Cipher.
E	Can be used for Message Authentication Codes.
F	Hardness based on factoring.
G	Hardness based on finding discrete logarithms.
H	Government Agency.
I	Pads plaintext messages.
J	Semantically secure.
K	Cryptographic attack.
L	Hash function.
M	Universally transitive secure.
N	Nonsense.