8. A

Design a python program to implement RSA Algorithm.

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP

key = RSA.generate(2048)
public_key = key.publickey()

cipher = PKCS1_OAEP.new(public_key)
encrypted = cipher.encrypt(b'Hello RSA')

cipher = PKCS1_OAEP.new(key)
decrypted = cipher.decrypt(encrypted)

print("Encrypted:", encrypted)
print("Decrypted:", decrypted.decode())
```

B

Design a C program to demonstrate Buffer overflow. And illustrate how it can be exploited by the attacker.

gets

```
#include <stdio.h>
#include <string.h>
int main() {
   void vulnerable();
   vulnerable();
   return 0;
}
void vulnerable() {
   char buffer[20];
   int passcheck = 0;
   printf("Enter the password: ");
   gets(buffer);
   if (strcmp(buffer, "nikhil123") == 0) {
      printf("Access Granted\n");
      passcheck = 1;
   } else {
      printf("Wrong password\n");
   }
   if (passcheck) {
      printf("You are allowed to work\n");
   }
}
```

Fgets

```
#include <stdio.h>
#include <string.h>

int main() {
   char password[16];
   int passcheck = 0;

   printf("Enter the password: ");
   fgets(password, sizeof(password), stdin);
   password[strcspn(password, "\n")] = '\0';

   if (strcmp(password, "nikhil123") == 0) {
      printf("Access Granted\n");
      passcheck = 1;
   } else {
      printf("Wrong password\n");
   }
   if (passcheck) {
      printf("You are allowed\n");
   }
   return 0;
}
```