9.1 Diffie-Hellman assumptions

9.1.a Bad Event Lemma on CDH

```
a, b ← Z_q

SEED():
  return (g^a, g^b)

CHECK(x):
  if x = (g^a)^b:
    return 1
  else:
    return 0
```

```
a, b ← Z_q

SEED():
  return (g^a, g^b)

CHECK(x):
  return 0
```

Because we know that for any given (g^a, g^b) an attacker cannot compute g^{ab} in polynomial time with non negligible probability, the advantage of any algorithm is also non-negligible. Therefore the two libraries are indistinguishable.

9.1.b Relation between DDH and CDH? What is the problem if one can solve CDH?

CDH is a "stronger" assumption than DDH, because one need to compute g^{ab} in non-negligible time, so therefore if CDH is solveable and non-negligible, the same can be said about DDH, so that it is not indistinguishable anymore. Therefore if one can solve the CDH in non-negligible time so is the discrete logarithm problem.

9.2 Man-in-the-middle attack

As ALICE will receive the wrong value $g^{b'}$ which was changed by EVE she will raise this to her chosen number a which will result in the key $(g^{b'})^a = g^{b' \cdot a}$. The same is happening to BOB who will calculate the key $(g^{a'})^b = g^{a' \cdot b}$.
Because the resulting keys are not equal, ALICE and BOB will not be able to decrypt the messages sent from one to the other (, *without any interception in between them*).
EVE can intercept the messages of ALICE and BOB. Because she/he can compute the keys which ALICE and BOB will have, by raising the intercepted g^a and g^b with either b' or a', she/he can decrypt the messages and encrypt them with the keys corresponding to ALICE or BOB. Therefore ALICE and BOB will not notice that anything is wrong, but EVE can read the sent messages.

9.3 Quadratic residues

We know that g is a *primitive root*, therefore it is:

$$\langle g \rangle_p = \mathbb{Z}_p^\star$$

We want to show that $g^a \in \mathbb{QR}_p^\star$ iff a is even. Suppose that this is true:

$$g^a \in \mathbb{QR}_p^\star \quad \Rightarrow \quad g^{a \cdot \frac{p-1}{2}} \equiv_p 1 \quad \Leftrightarrow \quad g^{\frac{a}{2} \cdot (p-1)} \equiv_p 1$$

Because a is even we can substitute $\frac{a}{2}$ with b which is still in $\mathbb{Z}$. Therefore we have:

$$g^{b \cdot (p-1)} \equiv_p 1 \qquad (1)$$

Because g is a *primitive root* of $\mathbb{Z}_p^\star$:

$$g^a \bmod p = g^{a+b \cdot (p-1)} \bmod p$$

Because $g^0 \equiv_p 1$, equation (1) is shown and therefore $g^a \in \mathbb{QR}_p^\star$.