1. RNG step:
    (a) The casino chooses prime number P and Q, and keeps them secret.
    (b) Then, the casino publishes N where N = P*Q. Also, the casino finds a X that is not a QR modulo N (which is easy for the casino) and publishes X. So (N,X) is the public key of the casino.
    (c) Each participant generates a 16 bits random number ($m_1m_2\cdots m_{16}$) and encrypts the number by:
    For each i, the participant randomly picks $y_i \in \{0, 1, \cdots, N-1\}$ such that gcd(y_i, n)=1. Then, the participant computes $c_i = y_i^2 * X^{m\_i}$ and sends c_i to the casino.
    (d) After a certain time T, the RNG system stops calling for participation.
    (e) Denote the c_i sent by player j as c_i^j . Denote the random number m sent by player j as m_j. Then, for each i, the casino computes $b_i = \Pi_j c_i^j$. And by decrypting b_i, the casino can get the xor of all the random number submitted by the participants, denoted as r'. (i.e. r'=m_1 xor m_2 xor ⋯)
    (f) The government sends the casino a random 16 bits number M. The casino computes r = r' xor M and uses r as the random number in the following steps.
2. The casino deposits. The casino can negotiate with the government and set an amount that both sides agree with. Only when the deposit reaches the amount can the casino start the bet. (In the sol, we store this amount in the variable "depositAmount" and assume it to be 1000 ether.)
3. The bettor deposits exactly 1 schilling and input a number k which is a random number chosen by the bettor. The contract records k and the player's address. k should not be a number that has been used in this day by the previous bettors. If k is a "losing number" that has been used by someone else already, it is the bettor's own responsibility to not to use it.
4. The casino receives k and check whether k has been used. If k has been used, the casino calls function "reportRepeatedNum" to refund the player. It is the casino's own responsibility to not let a "winning number" to be used more than once. (i.e. if someone reuses the "winning number" and the casino fails to detect this behavior and pays the bettor, the casino cannot ask the bettor to turn the money back even if later it is detected.) If not, the casino run rand(k+r) locally. Then, the casino announces whether the result is odd or even to the smart contract. The contract records the result. If the bettor wins, the contract pays the bettor 2 schilling. If the casino wins, the contract will keep the deposit from the bettor. The announce should be completed within due time, otherwise the bettor can get 2 schilling.
5. At the end of the day, the casino reveals r, P and Q. Then everyone verifies two things:
    (a) r is generated by the RNG step. (*)
    (b) For every k in the record of the smart contract, rand(k+r) should be the same as recorded.
6. If verification step(a) doesn't pass, the casino will pay all the players in both RNG game and gambling using its total deposit.

    If verification step(b) doesn't pass, the casino will pay those wronged bettors twice as much as their losses using its deposit.
7. If after T time, no one successfully reports a cheating, then the casino can call the function

to collect all the money in the smart contract.

(*): This verification step is actually a two-way verification. The RNG participants verify that the casino didn't temper the random numbers submitted by them. The casino wants to make sure the participants follow the step. (The participants may send a number directly to the casino, pretending this number to be a result from the encryption which is actually not. However, the number after decryption is not a uniformly distribution. Although one honest node can ensure the uniform randomness of the whole product, we do not encourage this kind of action and want to incentivize the players to follow the protocol.) The detailed step are as follows:

(a) Every RNG participant reveals their random number.

(b) The casino reveals P,Q and r. So now everyone can do the decryption and verification.

(c) The casino verifies that whether the random number revealed by the participants are corresponding to the c_i that they have submitted. If the participant passes the verification, he will get a reward. If the participant doesn't pass the verification, we will use the decryption result as his random number. However, he will not get rewarded.

(d) After decrypting all the random numbers, everyone can take xor of them (including M given by the government) and see whether the result is the same as r revealed by the casino. If they are not the same, then a cheating by the casino is detected.

Refinement:

1. From the above protocol, the casino can avoid loss by:

   When it sees someone submit number k that is going to win, it also creates a tx that submits number k, and bribes the miner.

   Solution: Use commitment scheme. The Player announce the hash value first, and after the contract records this player, the player announces his number.