HW 1 Cryptography

Andrew Johnson

1) Yes, this modified scheme should still have one time secrecy. It only takes away one possible option out of all the rest. It's also the trivial option. If λ isn't small the scheme is secure. $\frac{1}{2^\lambda} \approx \frac{1}{2^\lambda - 1}$.

2)

Query(2,5)	Query(2,5)
K ← KeyGen	K ← KeyGen
Enc(K,2)	Enc(K,5)

The left library will have an output of only even numbers in $\mathbb{Z}_{10}$, and the right library can only output 0 or 5. Therefore it would be easy to distinguish between libraries. since they have different probabilities.

3) Dec(K,C)
return (C-K)%n

Encrypt(K, m_L, m_R) ⇒ "
return (K+m_L)%n ⇒ return ctxt(K,m_L)

ctxt(K,m) ⇔ ctxt(K,m) so we can send in any m into ctxt since it wont use it
c ← (K+m)%n c ← $\mathbb{Z}_n$
return c return c

Encrypt(K,m_L,m_R) Return to the former ctxt and in line the code.
return ctxt(K,m_R)

Encrypt(K,m_L,m_R) ≡ Encrypt(K,m_L,m_R)
return (K+m_R)%n return (K+m_L)%n