HW1 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. $\frac{1}{2} \approx \frac{1}{2-1}$.

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 won't 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

9 people ABCDEFGHI

ABC DEF GHI

If we tried to use 6 out of 9 threshold then 2 groups can band together ie DEF-GHI get together and can break the code without anybody from ABC.

Since we need a majority from all groups then it must be 8 out of 9 because if it's 7 out of 9, you could have all of 2 subgroups and just 1 member from the last group, and 1 isn't a majority of that last group. 8 out of 9 is the only way to gaurntee what we want.