leungt30
Timothy Leung

# 1a

If you have enough plaintext and their corresponding ciphertext you can decipher any new plaintext that is a linear combination of previously known ciphertext.

For instance, if Trudy knows $E(k,1)$, and Alice sends an encrypted message $E(k,x)$. Then Trudy can decrypt $E(k,x)$ since $E(k,x) = E(k,1) + E(k,1) + \ldots + E(k,1) + E(k,1) = x * E(k,1)$. Since Trudy has the plaintext of $E(k,1)$ he also can decrypt $E(k,x)$.

# 1b

f(1E) = 72
f(00) = 63

$f(1E + 00) = f(1E) = 72$
$f(1E) + f(00) = 72 + 63 = D5$

$F(1E + 00)! = F(1E) + F(00)$
$\exists x, y | F(x + y) \neq f(x) + f(y)$

Therefore the S box is not a linear function

# 2

The has I got with the new function definitions is:
`a909986f702bf8d63dd741ff69ebb34c6ed957da07a9609322e43791edb7746b`

The SHA-256 implementation comes from https://github.com/keanemind/Python-SHA-256.

# 3

We start with $h_1$ is collision resistant and $h_2$ is not.

Suppose $h$ is not collision resistant, then we can find $x_1$ and $x_2$ such that $h(x1) = h(x2) = y||z$ since $h_2$ is not collision resistant then we can get $h_2(x1) = h_2(x_2) = z$.

But we also have access to all the bits before z, which I call y. This y is representative of the output of $h_1$ on $x_1$ and $x_2$ but since $h$ was not collision resistant, $h$ produces the same $y$ in $h(x_1)$ and $h(x_2)$. This proves $h_1$ is not collision resistant since $y = h_1(x_1) = h_1(x_2)$. Hence a contradiction.

Thus $h$ must be collision resistant.