ki	$zi(1)$
0	3
1	1
2	6
3	2
4	7
5	10

Travis Collins
ECE578 Lecture 5 Notes
October 1, 2012

1 Multiple Encryption

-Double encryption
Keyspace:$|K| = 2^k x 2^k = 2^{2k}$

$$x => encrypt => y => encrypt = y'$$

<u>Meet in the middle attack</u>

$$x => encrypt(k(i)) => z => encrypt(k(j)) => y$$

$$e_{ki}(x) = z_i^1 e_{kj}^{-1}(y) = z_j^(2)$$

Input: (x',y'),(x",y")
Idea: Compute

$$z_i^1 = e_{ki}(x)$$

$$z_j^2 = e_{kij}^{-1}(y)$$

Problem: Find $z_i^(1) = z_j^(2)$

Procedure:
1.) Compute lookup table $(z_i^{(1)}, k_i), i = 1, 2, ..., 2^k$
Storage: $2^k, (n + k)bits$
2.) Sort according to z_i column (Done typically while building table in step 1)

Values from the first encryption:

k	$zi(1)$
1	1
3	2
0	3
2	6
4	7
5	10

Use quick sort to look through table
Binary search: $log2(2^k) = k$ (iterations), k=keylength

3.) Find matching $z_j^{(2)}$
a.) Compute $e_{kj}^{-1}(y^1) = z_j^{(2)}$
b.) If

$$z_j^{(2)}$$

is in lookup table, i.e. $z_i^{(1)} = z_j^{(2)} => (k_i, k_j) -> try(x", y")(x''', y''')$
c.) If (k_i, k_j) give matchin encryption return (k_i, k_j) else goto 'a' try different

$$k_j$$

Complexity:
Brute Force: 2^{2k} encryptions (2x per iteration)
Meet in the middle attack: $Time = 2^k(Lookuptablei_values) + 2^k(onlinej_values)$

Triple encrytion:
Attack on first encryption (1)
$Time = 2^k + 2^{2k}$
$Space = 2^k$
Attack with second encryption (2)
$Time = 2^{2k} + 2^k$
$Space = 2^{2k}$

Question: How many additional pairs (x",y"), (x"',y"').... etc should we test?

Assume in general we have an encryption system with 'l' subsequence encryptions

Step1.)In step 1 we found a keypair such that $e_k...e_{kj}(e_{ki}(x')) = y'(lencryptions)$
There are 2^{lk} key combinations

How many possible values do I have for the cyphertext y' is $2^n(n = blocksize)$
One to one mapping x-¿y (2^n possible outputs), $2^{lk}/2^n numberofmappingspercipher text$

Number of keys that are found that are incorrect $2^{lk}/2^n - 1$

Step2.) We now use the candiadate key from step 1 and check if $e^l(x") = y"$

If a random key is used, the likelyhood that $e^l(x") = y"$ is $1/2^n$

If we check a third pair (x"',y"'), under the same random pair the probability will be:$1/2^{2n}$

If we check (t-1) additional pairs then the probability becomes $1/2^{(t-1)n}$

3.) Since there are $2^{lk}/2^n$ candidate keys in 1.) then probability that at least one fullfills all $e^l(x') = y', e^l(x") = y", ..., e^l(x'..') = y'..'$ is

$$(Numberofbadkeys)2^{lk}/2^n * 1/2^{(t-1)n}(probofpassingt - 1tests) = 2^{lk-tn}$$

Example: Double encryption with DES
k=56,n=64,l=2
if t=1, $Failure2^{112}/2^{64} = 2^48$