# Security Engineering – Quiz 2

Saturday April 2, 2016

## 3DES Encryption Technique

**Instructor -**

Dr. Sambuddho Chakravarty

**Submitted By -**

Deepak Kumar Sood

MT15013

MTech 1st year

**Question - Describe in a couple of paragraphs what is 3DES and how it differs from DES. Is there a particular attack that 3DES prevents? If so then please describe it.**

Answer -
**3DES** is a common name for Triple Data Encryption Algorithm is the successor to 2DES and DES which were rejected due to their known vulnerability. 3DES is a symmetric key block cipher which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

3DES uses 3 keys for all the 3 rounds of DES. The 3 rounds consists of encryption, decryption and then encryption.

## Keying Option:

There are 3 keying options provided in all the 3DES standards. They are:

1. **Keying option 1**

   All the keys are independent.

2. **Keying option 2**

   $K_1$ and $K_2$ are independent, and $K_3 = K_1$.

3. **Keying option 3**

   All three keys are identical, i.e. $K_1 = K_2 = K_3$.

Keying option 1 is the strongest, with $3 \times 56 = 168$ independent key bits.

Keying option 2 provides less security, with $2 \times 56 = 112$ key bits. This option is stronger than simply DES encrypting twice, e.g. with $K_1$ and $K_2$, because it protects against meet-in-the-middle attacks.

Keying option 3 is equivalent to DES, with only 56 key bits. It provides backward compatibility with DES, because the first and second DES operations cancel out.

## Algorithm:

Triple DES uses a "key bundle" that comprises three DES keys, $K_1$, $K_2$ and $K_3$, each of 56 bits (excluding parity bits). The encryption algorithm is:

$$\textbf{ciphertext} = E_{K3}(D_{K2}(E_{K1}(\textbf{plaintext})))$$

i.e., DES encrypt with $K_1$, DES *decrypt* with $K_2$, then DES encrypt with $K_3$.

Decryption is the reverse:

$$\textbf{plaintext} = D_{K1}(E_{K2}(D_{K3}(\textbf{ciphertext})))$$

I.e., decrypt with $K_3$, *encrypt* with $K_2$, then decrypt with $K_1$.

Each triple encryption encrypts one block of 64 bits of data.

In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.

**Basic difference between DES and 3DES -**

3DES uses 3 keys to encrypt, decrypt and encrypt the data block. It's like performing DES 3 times.

3DES provides effective security of 112 bits (key length) as opposed to 56 bits (key length) of security provided by DES.

3DES would take approximately 24 million year to bruteforce the key at 100M lookups per second while DES takes couple of days to bruteforce the key.

DES breaking times -

1997: Internet search -- 3 months

1998: EFF machine (deep crack) -- 3 days (250K $)

1999: combined search -- 22 hours

2006: COPACOBANA (120 FPGAs) -- 7 days

**Attack prevention by 3DES -**

- **Meet-in-the-middle attack (MITM attack) -**

MITM is a generic attack, applicable on several cryptographic systems.The Meet-in-the-Middle attack attempts to find a value using both of the range (ciphertext) and domain (plaintext) of the composition of several functions (or block ciphers) such that the forward mapping through the first functions is the same as the backward mapping (inverse image) through the last functions, quite literally *meeting* in the middle of the composed function.

The Multidimensional MITM (MD-MITM) uses a combination of several simultaneous MITM-attacks like described above, where the meeting happens in multiple positions in the composed function.

An exhaustive search on all possible combination of keys (simple brute-force) would take $2^{k \cdot j}$ attempts if *j* encryptions has been used with different keys in each encryption, where each key is *k* bits long. MITM or MD-MITM improves on this performance.

**Algorithm for MITM -**

- $SubCipher_1 = ENC_{f_1}(k_{f_1}, P),\ \forall k_{f_1} \in K$ :
  - and save each $SubCipher_1$ together with corresponding $k_{f_1}$ in a set A
- $SubCipher_1 = DEC_{b_1}(k_{b_1}, C),\ \forall k_{b_1} \in K$ :
  - and compare each new $SubCipher_1$ with the set A

When a match is found, keep $k_{f1}$,$k_{b1}$ as candidate key-pair in a table *T*. Test pairs in *T* on a new pair of *(P,C)* to confirm validity. If the key-pair does not work on this new pair, do MITM again on a new pair of *(P,C)*.

- **Bruteforce attack -**

This attack is not prevented in 3DES but due to its key size the complexity of the attack increases and also it takes a huge amount of time to bruteforce 3DES. Using today's hardware it would take 24 billion years to brute force 3DES which is practically not possible. Until now no known attack has been found. Therefore this is also prevented in 3DES.

## References -


https://en.wikipedia.org/wiki/Triple_DES

http://crypto.stackexchange.com/questions/25623/meet-in-the-middle-attack-on-3des

https://en.wikipedia.org/wiki/Meet-in-the-middle_attack

https://sites.google.com/site/sambuddhochakravarty/cse-3se-5se-winter-2016