Security Notions for Symmetric Key Encryption

Definition 1 (Security Against Key Recovery (KR))

Intuitively, this means that the knowledge of the Cipher Text must not allow adversaries to retrieve the key. In other words, should not leak out the key.

For example: If A and B are communicating and C is the adversary, who is learning the Cipher Text by some means. Then the Cipher text by no means should be able to reveal the key. Considering the adversary is a PPT (Probabilistic Polynomial Time algorithm), security notion should be resistive against brute force.

Formally, the notion of security against key recovery can be expressed using the following experiment between a PPT adversary and a challenger possessing the Shared Key.

$EXP_{SE}^{KR}(A)$

Where A is the Adversary, SE is Symmetric Key Encryption and KR is Key Recovery. Following is an Adversarial Game to explain the concept of Key Recovery

$k \leftarrow K \text{ from KeyGenerationAlgorithm}()$, $m \leftarrow M \text{ from Message space and } c \leftarrow ENC(m, k)$
1. The challenger challenges the adversary A on the Cipher Text produced by encrypting the message m using the random key k generated by key Generation Algorithm.

2. Adversary carries out certain operations which are bounded by polynomial time and sends back a guess of the key k’ to the challenger.

3. If adversary was able to crack the cipher text then a positive response ”1” is returned. Otherwise ”0” is returned.

Now, the probability of success of the experiment is the advantage of A to make the right ”guess for the key” is given by the following equation

\[ ADV_{SE}^{KR}(A) = PR(EXP_{SE}^{KR}(A) = 1) \]

SE is said to be secure against KR if

\[ \forall A \quad ADV_{SE}^{KR}(A) = neg(|k|) \]

the above expression states that for all adversaries who try to crack the scheme, Advantage is negligible function, that means least probability of success.

Where \(|k|\) is absolute value of k denoting the length of the key.

KR property is NECESSARY but not a SUFFICIENT condition. Why? Symmetric encryption can be secure against KR but may not be really secure. It could be revealing the Plain Text. Note that hiding the Plain Text is the primary/intuitive purpose of encryption.

We now look at the new notion of Security ”One Wayness” which is considered to be stronger than KR

**Definition 2 (One Way Security (OW))**

Intuitively this means that given a cipher text an adversary should not be able to retrieve the corresponding plain text.
Now, let us consider an experiment between PPT A and a challenger possessing the key, 

$$EXP_{SE^{OW}}(A)$$

where A is considered to be the adversary and the experiment is shown as follows.

1. The challenger challenges the adversary A on the Cipher Text produced by encrypting the message m using the random key generated by key generation algorithm $\text{Keygen}()$.

2. The adversary carries out certain operations which are bounded by polynomial time and sends back a guess of the message $m'$ to the challenger.

3. If the message $m'$, the plain text given by the adversary is same, then it returns a positive response '1'. Otherwise returns a '0' as a negative response.

Now, the probability of success of the experiment is the advantage of Adversary A, able to make the right guess for the message is given by the following equation:

$$ADV_{SE^{OW}}(A) = PR(EXP_{SE^{OW}}(A) = 1)$$

Now, SE is said to be OW secure if $\forall A$

$$ADV_{SE^{OW}}(A) = \text{neg}(n)$$

2-3
the above expression states that for all the adversaries who try to crack the scheme, the advantage is negligibly small. It has the least probability of success. Where "n" is considered a Security Parameter.

We now have looked into both KR and OW Securities, and its time to see which one is better among the two KR Vs OW

**Theorem :** \( (OW \Rightarrow KR) \) Any SE which is OW Secure will also be secure against KR.

**To Prove :** \( (\neg KR \Rightarrow \neg OW) \) Using contrapositive method we can prove that if SE is not secure against KR then it is also not OW secure. In other words if there exists one ‘A’ adversary who can break SE wrt KR, then we can construct another adversary ‘B’ who can break SE wrt OW.

B (adversary) is a reduction given A (adversary)

**Given :** A who is capable of breaking SE wrt KR.

Following is the diagram which shows the way one wayness calls KR to break OW security

1. The challenger challenges the adversary B on the Cipher Text produced by encrypting the message m from the message space using the random key generated by key generation algorithm ()

2. The adversary B pass the Cipher Text ”c” to the adversary A, where A assumes that it is communicating with the KR challenger.

3. The adversary carries out certain operations which are bounded by polynomial time and reply back with a guess of the key k’ to the adversary B.
4. The adversary B decrypts Cipher Text “c” using the key k’ to obtain m’

5. The adversary B send m’ as a reply back to the challenger.

6. If the message m’ given by the adversary is same, then it returns a ’1’ else returns a ’0’.

**Probability of Success is:**

\[
ADV_{SE}^{OW}(B) = PR(EXP_{SE}^{OW}(B) = 1)) \\
ADV_{SE}^{OW}(B) = PR(m’ = m) \\
ADV_{SE}^{OW}(B) = PR(DEC(c, k’) = m) \\
ADV_{SE}^{OW}(B) = PR(k’ = k) \\
ADV_{SE}^{OW}(B) = PR(EXP_{SE}^{KR}(A) = 1)
\]

Which Implies

\[
ADV_{SE}^{OW}(B) = ADV_{SE}^{KR}(A)
\]

From the above proof of the theorem we can infer that any scheme which is OW secure would automatically be secure against KR, thus OW exhibits a stronger property compared to the KR

*Let us Check: Is the converse of the above mentioned theorem true, that is mathematically does KR ⇒ OW*

The answer to the above question is **NO**, KR does not ⇒ OW the converse does not hold good, which means that every encryption scheme that is secure against KR is not necessarily OW secure. To prove the above claim we have to come up with an example where we have an encryption scheme that outputs the Cipher Text similar to the plain text which is shown here

\[c = ENC(m, k)\]

where c is encrypted with k, it again gives out c which is same like m and does not give out any information about the key k.Here k is not broken but m is revealed because cipher is less secure and is similar to m.

*Is OW security a necessary and a sufficient property? YES, it is a necessary property but not a sufficient property for the security of an Encryption scheme.*
It is not sufficient enough because a part of the message is leaked out which may be the most important part of the message.

For example if two parties are communicating with each other and there are possibilities that the user might learn partially something from the message and the partial message that has leaked out might be the most important part of the message.

Now that this is not perfectly secure and sufficient enough this gives us an opportunity to look into the next topic called SEMANTIC SECURITY.

**Definition 3 (Semantic Security)**

This security relates to the Perfect Security. Intuitively, a SE is said to be *SEMANTIC* secure if the Cipher Text does not reveal "Anything" about the Plain Text.

In the above diagram “f” is a deterministic function and “y” is a value such that $y = f(m)$. The experiment returns “1” if $y = f(m)$. Otherwise returns “0”.

A SE is called SEM if $\forall A$

$$ADV_{SE}^{SEM}(A) = neg(n)$$

If the adversary A wins with a negligible probability then the scheme is said to be SEMANTICALLY SECURE.
**Definition 4 (Indistinguishability (IND))**

Intuitively, a SE scheme is said to exhibit IND property if given a cipher text of one of the two messages, it should be **"HARD"** for the adversary to Guess the "Cipher Text" correspond to which of the two Messages.

For example when two messages \(m_0\) and \(m_1\) are given to the adversary, its hard to relate the message to the corresponding cipher text.

The Indistinguishability property relates to the *Third Definition from our First Lecture*

Which was like this:

\[
\text{PR}(C = c| M = m_0) = \text{PR}(C = c | M = m_1) \approx \text{PR}(C = c | M = m_0) = \text{Neg}() \text{ (Close Enough to conclude)}
\]

*Following is the experiment to explain the concept of Indistinguishability.*

The challenger either resides in WORLD-1 or WORLD-0 and both are independent of each other.

**World 1**

1. The Adversary picks two messages \(m_1, m_0\) randomly from the message space and send them to the challenger.

2. In the **WORLD-1**, the challenger encrypts \(m_1\) using the random key \(k\), and send the corresponding cipher text \(c\) to the Adversary.

3. The Adversary now comes up with a guess "\(d\)" in order to find out if message \(m_1\) or message \(m_0\) was encrypted and send it back to the challenger.
Advantage for World-1

\[ ADV_{SE}^{IND}(A) = PR(EXP_{SE}^{IND^{-1}}(A) = 1) \]

Experiment at World-0

1. The Adversary picks two messages \( m_1, m_0 \) randomly from the message space and send them to the challenger.

2. In the WORLD-0, the challenger encrypts \( m_0 \) using the random key \( k \), and send the corresponding cipher text \( c \) to the Adversary.

3. The Adversary now comes up with a guess ”d” in order to find out if message \( m_1 \) or message \( m_0 \) was encrypted and send it back to the challenger.

Advantage for World-0

\[ ADV_{SE}^{IND}(A) = PR(EXP_{SE}^{IND^{-0}}(A) = 1) \]

Probability of Success/Advantage of the Indistinguishability Property

\[ ADV_{SE}^{IND}(A) = PR(EXP_{SE}^{IND^{-1}}(A) = 1) - PR(EXP_{SE}^{IND^{-0}}(A) = 1) \]

The Above Equation can alternatively be written as:

\[ ADV_{SE}^{IND}(A) = PR(EXP_{SE}^{IND^{-1}}(A) = 0) - PR(EXP_{SE}^{IND^{-0}}(A) = 0) \]

SE is called IND if \( \forall A, \)

\[ ADV_{SE}^{IND}(A) = Epsilon \]

Definition 5 (Indistinguishability Guess (IND-G))

Here the adversary A tries to guess which bit was used to encrypt.

\[ EXP_{SE}^{IND-G}(A) \]
Experiment for Indistinguishability-Guess

1. The adversary picks two messages $m_1$ and $m_0$ randomly from the message space $M$ and send them to the challenger.

2. The challenger encrypts either of the messages using the randomly generated key $k$ and sends the corresponding cipher text $c$ to the Adversary. In this case the message could be "0" or "1".

3. The Adversary now comes up with a guess $b'$ in order to find out if message $m_0$ or message $m_1$ was encrypted and sends the $b'$ back to the challenger.

Probability of Success/Advantage of the Indistinguishability Guess Property

$$\text{ADV}_{SE}^{IND-G}(B) = PR(\text{EXP}_{SE}^{IND-G}(A) = 1))$$

SE is said to be IND-G secure if $\forall A,$

$$\text{EXP}_{SE}^{IND-G}(A) = 1/2 + Epsilon$$

the probability of 1/2 is always included because the adversary can always make a correct guess with a probability 1/2.

**Theorem**: $(IND \iff IND - G)$

Considering: $(\neg IND \Rightarrow \neg IND - G)$

**Proof**: If there exist Adversary A, who can break SE against IND then we can construct Adversary B who can break SE against IND - G.
The adversary A picks two messages m0, m1 and send them to adversary B and then B pass it to the challenger. Now the challenger picks any Bit and encrypt the message mb using random key k generated by a key generation function. This Cipher Text is send ack to adversary B and B pass it to the adversary A. Adversary A bounce back with the ”guess” d and pass it on to the adversary B. B respond to the challenger with a decrypted bit b'.

Advantage of adversary A using IND:

\[
ADV_{SE}^{IND}(A) = PR(EXP_{SE}^{IND-1}(A) - PR(EXP_{SE}^{IND-0}(A) = 1))
\]

The probability of success of the adversary is given by:

\[
ADV_{SE}^{IND-G}(B) = PR(b' = b)
= PR(b' = 1 \text{ AND } b = 1) + PR(b' = 0 \text{ AND } b = 0)
\]

now, applying Baye’s Theorem:

\[
PR(A/B) = Pr(A \text{ AND } B)/PR(B)
PR(A \text{ AND } B)=PR(A/B).PR(B)
\]

Now,

\[
ADV_{SE}^{IND-G}(B) = [PR(b' = 1|b = 1).PR(b = 1)] + [PR(b' = 0|b = 0).PR(b = 0)]
\]
\begin{align*}
&= 1/2[PR(b' = 1|b = 1) + PR(b' = 0|b = 0)] \\
&= 1/2[PR(b' = 1|b = 1) + 1 - PR(b' = 1|b = 0)] \\
&= 1/2[1 + PR(b' = 1|b = 1) - PR(b' = 1|b = 0)] \\
&= 1/2[1 + ADV_{SE}^{IND}(A)]
\end{align*}

\[ADV_{SE}^{IND}(A) = 2ADV_{SE}^{IND-G}(B) - 1 = \text{EPSILON}\]