CSA E0 235: Cryptography January 18, 2016

Scribe for Lecture 4

Instructor: Arpita Patra *Submitted by: Shipra Chauhan*

1 Overview

With the basic understanding of the definition of Perfect Security , we have figured out the limitations regarding its feasibility in practical usage. We are aware that we can not afford a key of size same as the size of the message to be encrypted and that too can be used only once. So in order to ensure smooth implementation of security the definition of Perfect Security was relaxed and hence Computational Security was introduced.

Coming to the question of what is relaxed and why is that relaxation required ?
The definition of Computational Security is based on two relaxations of the notion of Perfect Security:

- Security is only preserved against ***efficient*** (computationally bounded) adversaries.
- Adversaries can potentially succeed with some ***very small probability*** (negligible).

The answer to why relaxation is required will become clear as we move forward and consequently the concept of **Concrete Approach** and **Asymptotic Approach** for computational security will be introduced followed by the definitions and significance of **Semantic Security** and **Indistinguishability Security**.

2 Necessity of Relaxations

2.1 Necessity of relaxed Threat Model

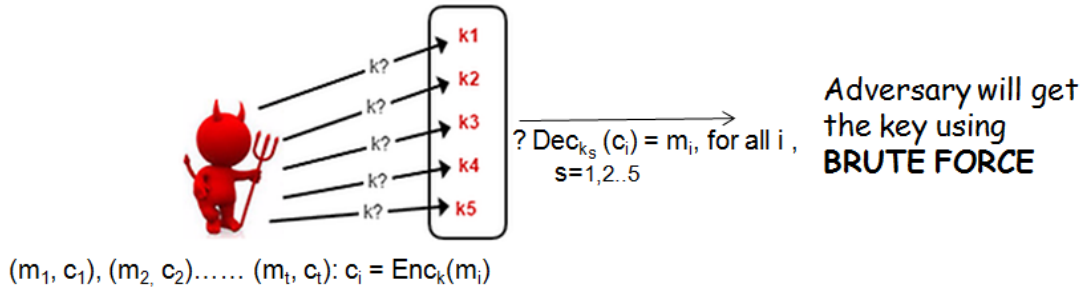

Figure 1: Experiment for relaxed Threat Model

The relaxations are actually done to eliminate the limitations of Perfect Security as discussed above. The following mentioned experiment will make the complete scenario logical, that how the concept of using the single short key for encrypting multiple messages demand the limit on unbounded computational power given to adversary in order to promise intact security.

Assume an adversary with unbounded power in contrast to bounded and he knows many message and cipher text pairs as shown in Figure 1. Considering these pairs $(m_1, c_1), (m_2, c_2)$ .....(m_t, c_t) : $c_i = Enc_k(m_i)$,the aim of adversary is to get the correct key. With his unbounded computational power he will decrypt each cipher text with all possible keys until he finds the correct matching key for which $Dec_k(c_i) = m_i$ for all i. This Brute Force Search will take $O(|\mathcal{K}|)$.

To encrypt many messages using a single short key, security can only be achieved if we limit the running time of the adversary such that he can not carry out a fruitful brute force search.

2.2 Necessity of relaxed Break Model

Proceeding with assumptions made in the threat model, many messages need to be encrypted using a single, short key. Unlike Perfect Security where it was impossible to break, here it is infeasible to break with high probability. Adversary has many message and cipher text pair and chooses a single key randomly. The time taken will be $O(1)$ with negligible probability of success, $1/|\mathcal{K}|$. Figure 2 illustrates the guessing experiment for relaxed Break Model which signifies that the probability required to break our cryptosystem by any such adversary should be negligibly small.

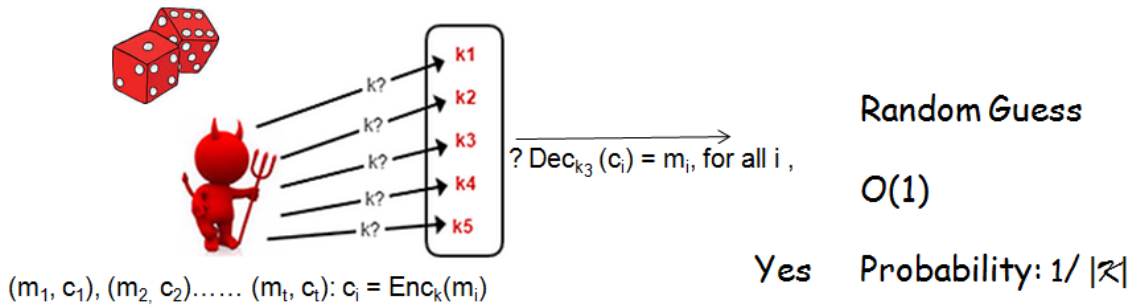

Figure 2: Experiment for relaxed Break Model

Why not Concrete but Asymptotic Approach !!!

The Concrete Approach gauzes the security of a given cryptographic scheme by bounding the maximum success probability of any adversary running for at most some specified amount of time. A scheme is (t, ε) secure if every adversary running for time at most t succeeds in breaking the scheme with probability at most ε where t, ε are positive constants with $\varepsilon \leq 1$. Theoretically, this approach is disadvantageous since schemes can be (t, ε) *secure* but never just *secure*. For what ranges of t, ε should we say that a (t, ε) secure scheme is secure? There is ambiguity to its answer, as a security guarantee that may suffice for the average user may not suffice when encrypting classified government documents. Also with the rapid development in the computer architecture, we can not construct the security scheme against specific system with estimated break time. If adversary gets more powerful machine then entire system need to be reconstructed which is not all desirable. So we work with Asymptotic Approach, which rooted in complexity theory, views the running time of the adversary as well as its success probability as functions of some parameter rather than as concrete numbers.

3 Asymptotic Approach

Kerckhoffs is best known for his principle that cryptographic designs should be made public. According to one of his principles, ***A cipher must be practically, if not mathematically, indecipherable***[1].This symbolizes that it is not necessary to use a perfectly-secret encryption scheme, but instead it suffices to use a scheme that cannot be broken in reasonable time with any reasonable probability of success, a scheme that is practically indecipherable.

3.1 Polynomially Bounded Asymptotic Approach

According to this scheme the Adversary is polynomially bounded means it can run only Probabilistic Polynomial Time(PPT) algorithms. We can define a polynomial function as a function $f : Z^+ \rightarrow Z^+$ is polynomial in n if there exist finite number of c_i such that $f(n) < \sum_i c_i n_i$ for all n. Example: n^3.

Now the question is that how much can this PPT adversary handle?
An efficient/PPT adversary **cannot** brute-force over $\mathcal{K}$, if value of $\mathcal{K}$ is adjusted properly. Here $\mathcal{K}$=2^n, n bits signifies the size of your key. So regulating the value of n such that it does not create difficulty for adversary.

3.2 Negligible Asymptotic Approach

We equate the notion of **small probability of success** with success probabilities smaller than any inverse-polynomial in n, meaning that for every constant c the adversary's success probability is smaller than $1/n^c$ for large enough values of n, these kind of functions are

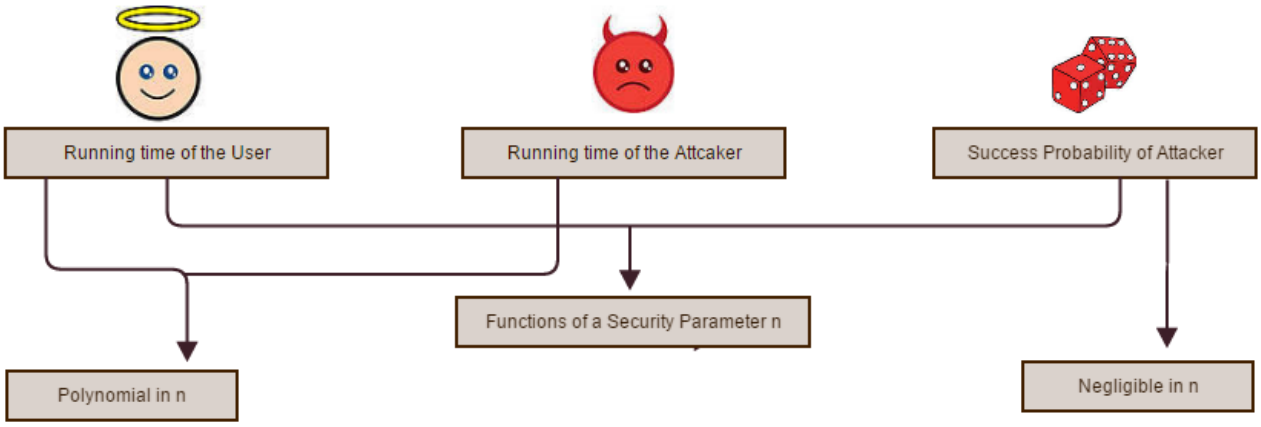

Figure 3: Asymptotic Approach at a glance

negligible functions that grow slower than any inverse polynomial. In other words for every polynomial in $n, p(n)$, there exists some positive integer N, such that $f(n) < 1/p(n)$, for all $n > N$. For example an adversary running for n^3 time breaks a scheme with probability at most $1/2^n$. So it can be inferred that increasing the value of n will cause sturdy brute force, successively augmenting the pain for adversary. Figure 3 illustrates Asymptotic Approach more clearly.

3.2.1 Closure properties of Polynomial and Negligible Functions

Polynomial Functions are closed under addition and multiplication operations i.e.If p_1 and p_2 be polynomials in n then,

- $p_1 + p_2$ is a polynomial.
- $p_1 * p_2$ is a polynomial.

Negligible functions are closed under following operations, assuming that $negl_1$ and $negl_2$ are negligible functions in n then,

- $negl_1 + negl_2$ is a negligible function.
- $p(n).negl_1$ is a negligible function for any polynomial $p(n)$

EXCITING FACTS ☺

- Physicists believe that the no. of seconds elapsed since the birth of Earth is in the order of 2^{58}.
- Something that occurs with probability 2^{-60}/sec is expected to occur once every 100 billion years.

n : SECURITY PARAMETER
n is a tunable parameter that tunes how difficult it is to break a cryptosystem. But we cannot set n to arbitrarily large values and get ultimately powerful cryptosystems as the key size is usually set equal to n. Therefore raising the value of n randomly will increment the running time of user. So value of n should be chosen carefully for promising cryptosystem. e.g. A designer claims that an adversary running for n^3 minutes can break his scheme with probability $2^{40}2^{-n}$, where $2^{40}2^{-n}$ is negligible function but value of n will act as deciding factor.

- If $n <= 40$, break time: 6 weeks, probability : 1
- If $n = 500$, break time: 200 yrs, probability: 2^{-460}

Value of n depends on demand of particular cryptosystem.

4 Semantic Security for SKE

Semantic Security encapsulates the perception that except the prior information about message, the cipher text does not reveal any new information about the original message.Thus, **the notion of semantic security is the computational equivalent of the notion of perfect secrecy**.

Definition 1[1] *An encryption scheme π = (Gen,Enc,Dec) is semantically secure if, for every PPT algorithm $\mathcal{A}$, and polynomial-time computable functions $f()$ and $h()$, there exists another PPT algorithm $\mathcal{A}'$ such that*

$$| \mathbb{P}[\mathcal{A}(1^n, Enc_k(m), h(m)) = f(m)]_{\substack{k \leftarrow Gen(1^n) \\ m \in_R \mathcal{M}}} - \mathbb{P}[\mathcal{A}'(1^n, |m|, h(m)) = f(m)]_{m \in_R \mathcal{M}} | \quad (1)$$

is negligible $\diamondsuit$

We try to foresee the definition with the scenario where we consider two PPT adversaries $\mathcal{A}$ and $\mathcal{A}'$.The aim of these adversaries is to find the message $f(m)$. Both are provided with some prior information about the message which is encrypted, calling this function as $h(m)$(history function). Now we provide the ciphertext $Enc_k(m)$ only to adversary $\mathcal{A}$ and the value of $|m|$ is given to adversary $\mathcal{A}'$ as shown in Figure 4. The scheme is semantically secure if the difference between the probabilities of guessing $f(m)$ by $\mathcal{A}$ and $\mathcal{A}'$ is negligible. This illustrates that how access to cipher text can not make any noticeable change in the probability of guessing the additional information $f(m)$.

5 Indistinguishability Security for SKE

The concept of Indistinguishability clears a very vital point for strong security, given the knowledge of two messages, it cannot be distinguished if the ciphertext corresponds to the

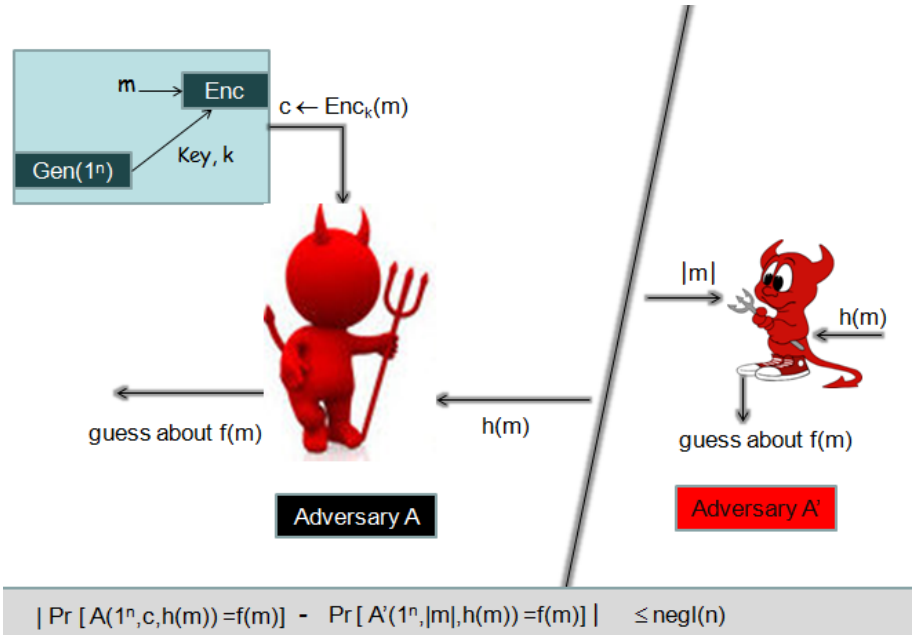

Figure 4: Experiment for Semantic Security

first or second message. We assume the COA(Ciphertext Only Attack) where adversary can have access of ciphertext and nothing else.

Definition 2[1] A private-key encryption scheme π = (Gen,Enc,Dec) has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there exists a negligible function *negl* such that

$$| \ Pr[PrivK^{ind}_{\mathcal{A},\pi}(n) = 1] \ | \leq \frac{1}{2} + negl(n) \tag{2}$$

where the probability is taken over the random coins used by $\mathcal{A}$, as well as the random coins used in the experiment (for choosing the key, the random bit b, and any random coins used in the encryption process). ♢

Introducing an experiment for comprehension of the logic of Indistinguishability.

- The adversary $\mathcal{A}$ is given input 1^n, and outputs a pair of messages m_0, m_1 of the same length as can be seen in Figure 5.
- Challenger runs Gen(1^n) to produce a random key k, and then flips a coin to select random bit b ←0,1 according to which the selected message is encypted and the ciphertext c ←$Enc_k(m_b)$ is forwarded to $\mathcal{A}$.
- In return adversary $\mathcal{A}$ outputs a bit b' by guessing about encrypted message. If b' = b, then output is given as 1 i.e. $PrivK^{ind}_{\mathcal{A},\pi}(n) = 1$, we say $\mathcal{A}$ succeeds otherwise $\mathcal{A}$ loses.

5.1 Indistinguishable COA security

The above defined expression can be validly formulated for Ciphertext Only Attack where we consider the PPT adversary. Here the system in not impossible to break but infeasible to break with high probability which is adequate for practical security systems. Probability is taken over the randomness used by the Adversary and Challenger.

Definition 3 A symmetric-key encryption scheme is said to be IND-COA secure (i.e. has indistinguishable encryptions under ciphetext-only attack) if, for every PPT adversary $\mathcal{A}$,

$$Pr[PrivK^{coa}_{\mathcal{A},\pi}(n) = 1] \leq \frac{1}{2} + negl(n) \tag{3}$$

$\diamondsuit$

This definition is the valid evidence that even when adversary $\mathcal{A}$ has two messages m_0, m_1 and ciphertext of one of m_0 and m_1, he can not effectively distinguish the correct message corresponding to the given cipher text.

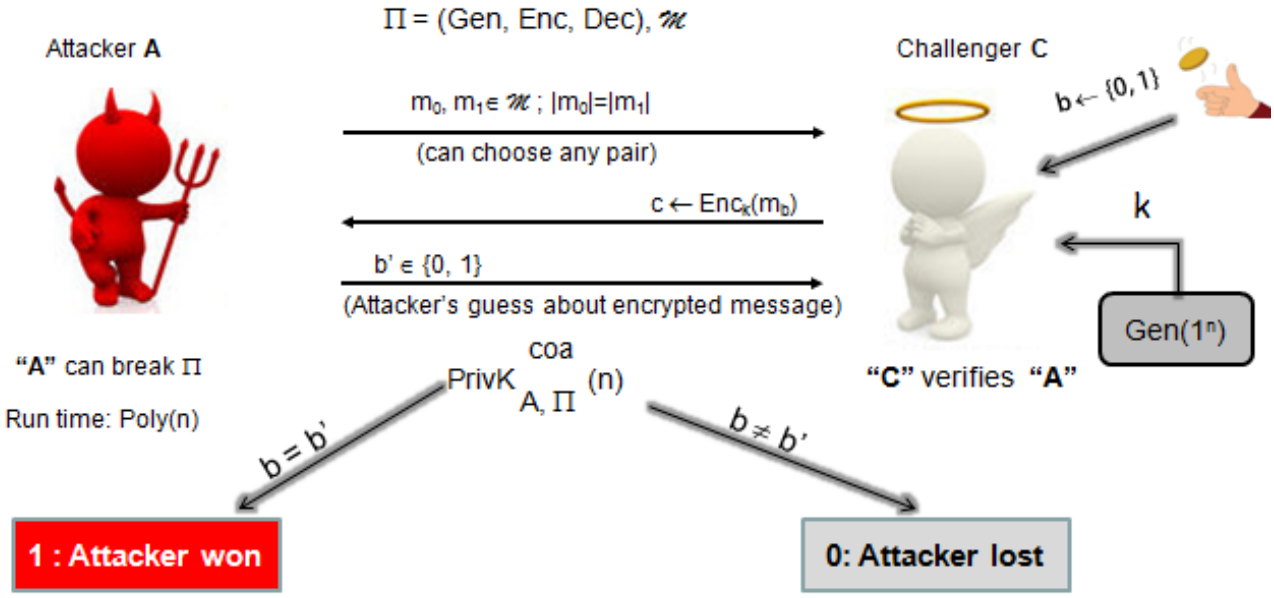

Figure 5: Experiment for Indistinguishability Security

Equivalence of Semantic and Indistinguishablity Security This can be seen intutively that the Semantic and Indistinguishablity Security are equivalent. We say adversary cannot detect which plaintext was encrypted with advantage significantly better than taking a random guess.In other words for any message m_0, m_1 which are of same length, he outputs 1 with almost the same probability in each case i.e Adversary behaves in the same way irrespective of m_0 or m_1. Thus we can formulate another equivalent definition.

Definition 4 A private-key encryption scheme π = (Gen,Enc,Dec) has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there exists a negligible function negl such that

$$|Pr[output(PrivK^{ind}_{A,\pi}(n,0)) = 1] - Pr[output(PrivK^{ind}_{A,\pi}(n,1)) = 1]| \leq negl(n) \quad (4)$$

♢ [1]

WHY RANDOMNESS ??
Computational Security took birth to eliminate the limitations of Perfect Security (One Time Pad 6).i.e. necessity of short and reusable key to make cryptosystem practical. In cases when the length of a message might itself represent sensitive information (number of digits in an employee's salary), care should be taken to pad the input to some fixed length before encrypting.
We can not simply mask the message with key only, but randomness is required. Certain functions can be applied accordingly on key to get better padding in terms of length which increases the randomness till some level. Besides this, feasibility should be reatined therefore as we consider computational security it is enough if the pad *looks* random to a PPT adversary but actually not. This lead to the notion of Pseudorandomness which is elementary for cryptography.

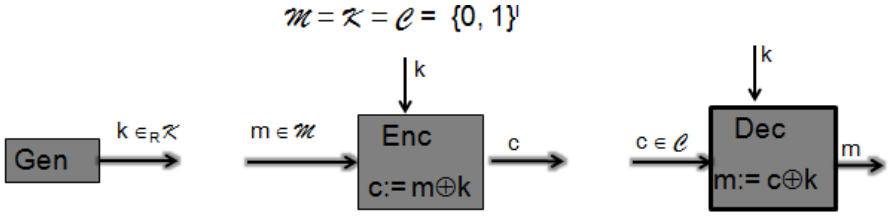

Figure 6: One Time Pad Scheme

6 Pseudorandomness

Pseudorandomness plays a fundamental role in cryptography in general, and private-key encryption in particular. This can be entitled as a property of probability distribution.When an entity runs in polynomial time , the pseudorandom string looks like a uniformly distributed string. Just as indistinguishability can be viewed as a computational relaxation of

perfect secrecy, pseudorandomness is a computational relaxation of true randomness. For clearer view figure 7 can be referred where we consider a probability distribution G and a uniform probability distribution U. Now G is pseudorandom if a PPT distinguisher can not distinguish between the string drawn according to G and a string drawn according to U.

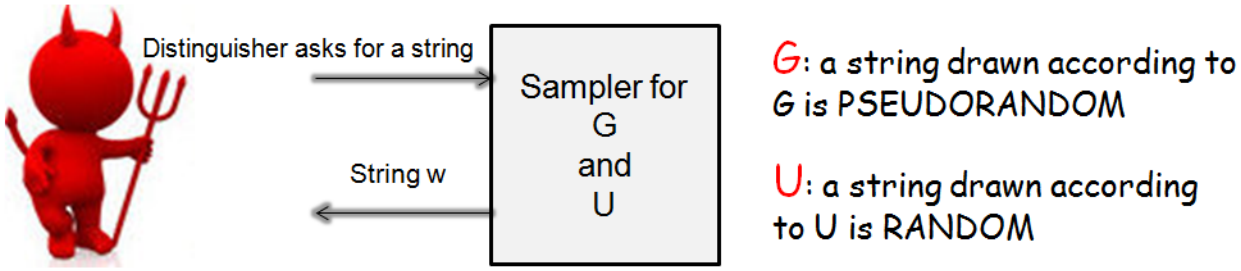

Figure 7: Pseudorandomness

Now we are familiar with the idea of computational security, what kind of relaxations and the requirement of these relaxations, why we choose Asymptotic Approach and the concept of negligible function followed by the Semantic and Indistinguishablility Security and their equivalence, and lastly the importance of randomness in cryptography therefore evolution of Pseudorandomness took place. We will next look in to the pseudorandom genarators which will give another dimension to cryptography.

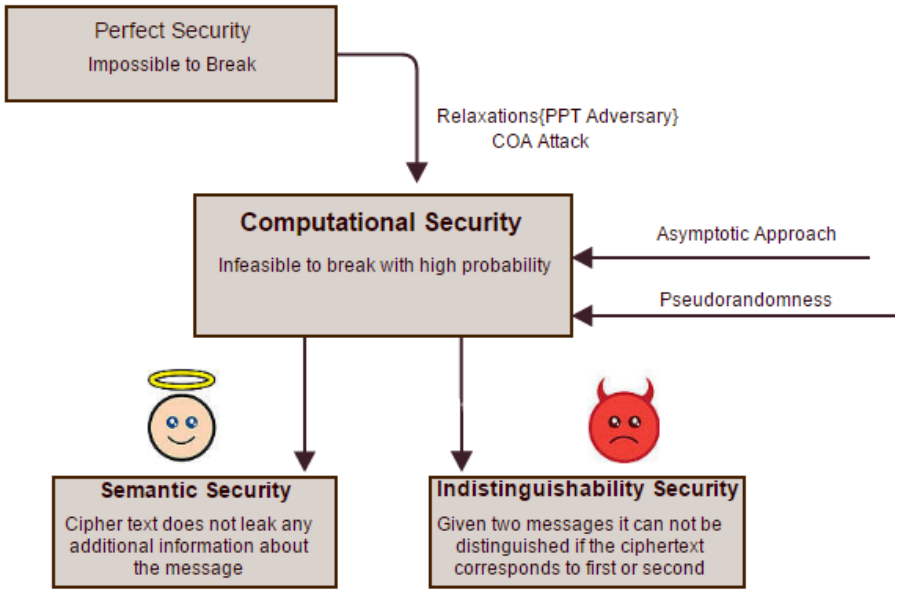

Figure 8: Overview

References

[1] Katz, Jonathan, and Yehuda Lindell. *Introduction to modern cryptography.* CRC Press, 2014.

[2] Arpita Patra. *http://drona.csa.iisc.ernet.in/∼arpita/Cryptography16.html.* Course Materials.