Cryptography - The Journey Begins

Nilanjan Datta

Institute for Advancing Intelligence, TCG CREST, Kolkata

CREST CRYPTO Summer School 2025, Kolkata

tcg crest
Inventing Harmonious Future

Cryptography

cryptography *noun*

/krɪp'tɒgrəfi/

/krɪp'tɑːgrəfi/

[uncountable]

- the art of writing or solving codes

Cryptography

cryptography *noun*

/krɪp'tɒgrəfi/

/krɪp'tɑːgrəfi/

[uncountable]

the art of writing or solving codes

Cryptology = Cryptography + Cryptanalysis

The Basic Set up

Alice

Bob

The Basic Set up

Alice

Messages

Bob

The Basic Set up

Eve

Messages

Alice

Bob

Notion of An Adversary

- Passive Adversary: Observes the Message
- Active Adversary: Modifies the Message

Why Cryptography?

My Netflix password is ND180722

Why Cryptography?

My Netflix password is ND180722

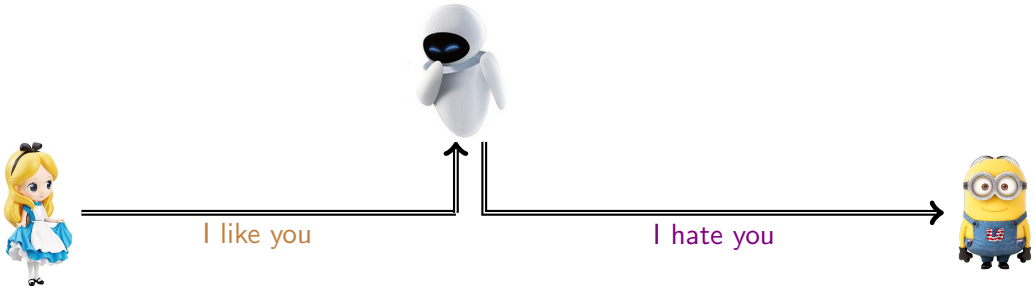
We need Confidentiality

- Bob should read the message.
- Eve should not read the message.

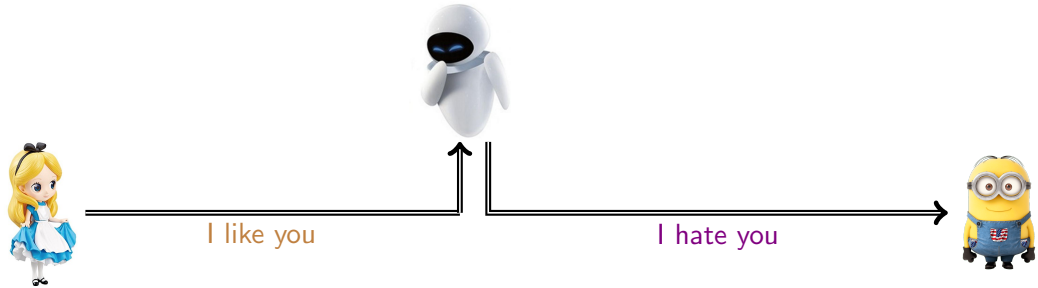
Why Cryptography?

I Like you

Why Cryptography?



Why Cryptography?



We need Authentication/Integrity

Bob should be able to validate the authenticity of the message and the integrity of Alice.

Why Cryptography?

@ * # * *#$$ * # * *@

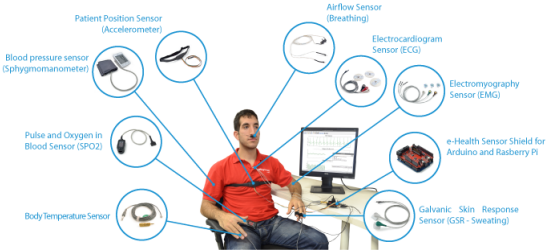
Why Cryptography?

@ ∗ # ∗ ∗ # $$ ∗ # ∗ ∗ @

We need Non-Repudiation

Alice can not deny a message that she sent to Bob.

Real-Life Applications



Cryptography

Symmetric-Key Cryptography

Alice and Bob share a secret key.

Cryptography

Symmetric-Key Cryptography

Alice and Bob share a secret key.

Public-Key Cryptography

Each User has a public key and a secret key.

Symmetric-Key Encryption

Message Space: $\mathcal{M}$, Ciphertext space: $\mathcal{C}$, Key-space $\mathcal{K}$.

- Keygen: $K \leftarrow_{\$} \mathcal{K}$.
- Encryption: $C \leftarrow Enc_K(M)$.
- Decryption: $M := Dec_K(C)$.

Symmetric-Key Encryption

Message Space: $\mathcal{M}$, Ciphertext space: $\mathcal{C}$, Key-space $\mathcal{K}$.

- Keygen: $K \leftarrow_{\$} \mathcal{K}$.
- Encryption: $C \leftarrow Enc_K(M)$.
- Decryption: $M := Dec_K(C)$.

Correctness: For any M, K, $Dec_K(Enc_K(M)) = M$.

Kerckhoffs' Principle

- The cryptosystem is known to the adversary.
- But the key is not known to the attacker.
- The secrecy of the cryptosystem lies in the key.

Public-Key Encryption

Receiver's Key: $(R.PK, R.SK)$

- Encryption: $C \leftarrow Enc_{R.PK}(M)$.
- Decryption: $M := Dec_{R.SK}(C)$.

Public-Key Encryption

Receiver's Key: $(R.PK, R.SK)$

- Encryption: $C \leftarrow Enc_{R.PK}(M)$.
- Decryption: $M := Dec_{R.SK}(C)$.

Correctness: For any $M, (U.PK, U.SK)$, $Dec_{U.SK}(Enc_{U.PK}(M)) = M$.

Historic and Classical Ciphers

The "Art" of Message Hiding

The “Art” of Message Hiding

Ohw wkh Jdph Ehjlq..

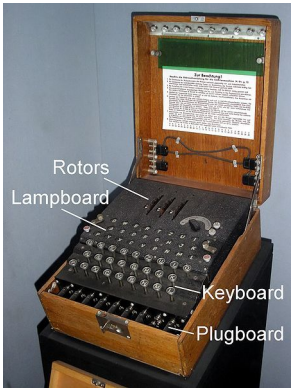
The "Art" of Message Hiding

Ohw wkh Jdph Ehjlq..

The "Art" of Message Hiding

Historic Ciphers: Enigma Machine

https://www.youtube.com/watch?v=ybkkiGtJmkM



Classical Ciphers

Shift Cipher

$\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$.

- Keygen: $K \leftarrow_{\$} \mathbb{Z}_{26}$.
- Encryption: $C := (K + M) \mod 26$.
- Decryption: $M := (K + C) \mod 26$.

Shift Cipher - Cryptanalysis

Can you decipher the following text?

JBCRCLQRWCRVNBJENBWRWN,

Shift Cipher - Cryptanalysis

Can you decipher the following text?

JBCRCLQRWCRVNBJENBWRWN,

After applying brute force search:

jbcrclqrwcrvnbjenbwrwn
iabqbkpqvbqumaidmavqvm
hzapajopuaptlzhclzupul
gyzozinotzoskygbkytotk
fxynyhmnsynrjxfajxsnsj
ewxmxglmrxmqiweziwrmri
dvwlwfklqwlphvdyhvqlqh
cuvkvejkpvkogucxgupkpg
btujudijoujnftbwftojof
astitchintimesavesnine

Affine Cipher

$\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}$, $\mathcal{K} = \mathbb{Z}_{26}^{\star} \times \mathbb{Z}_{26}$.

- Keygen: $(K_1, K_2) \leftarrow_{\$} \mathbb{Z}_{26}^{\star} \times \mathbb{Z}_{26}$.
- Encryption: $C := (MK_1 + K_2) \mod 26$.
- Decryption: $M := K_1^{-1}(C - K_2) \mod 26$.

Affine Cipher

$\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}$, $\mathcal{K} = \mathbb{Z}_{26}^{\star} \times \mathbb{Z}_{26}$.

- Keygen: $(K_1, K_2) \leftarrow_{\$} \mathbb{Z}_{26}^{\star} \times \mathbb{Z}_{26}$.
- Encryption: $C := (MK_1 + K_2) \mod 26$.
- Decryption: $M := K_1^{-1}(C - K_2) \mod 26$.

How to cryptanalyze affine cipher?

Substitution Cipher

$\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}$, $\mathcal{K} = \mathbb{P}(26)$.

- Keygen: $\pi \leftarrow_{\$} \mathbb{P}(26)$.
- Encryption: $C := \pi(M)$.
- Decryption: $M := \pi^{-1}(C) \mod 26$.

Cryptanalysis of Substitution Cipher

Can you decipher the following text?

```
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Cryptanalysis of Substitution Cipher

Can you decipher the following text?

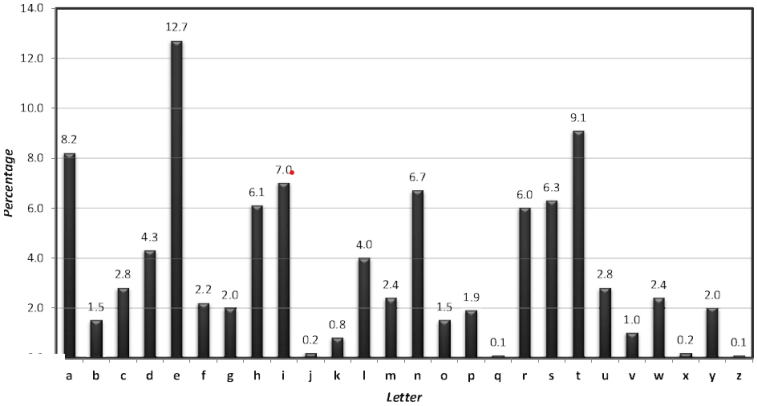
```
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

How about applying a brute-force search?

Cryptanalysis of Substitution Cipher

Cryptanalysis of Substitution Cipher

Use Frequency Table:



Cryptanalysis of Substitution Cipher: Frequency Table

```
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

letter	frequency	letter	frequency
A	0	N	9
B	1	O	0
C	15	P	1
D	13	Q	4
E	7	R	10
F	11	S	3
G	1	T	2
H	4	U	5
I	5	V	5
J	11	W	8
K	1	X	6
L	0	Y	10
M	16	Z	20

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$
- C, D, F, J, M, R, Y might be encryptions of t, a, o, i, n, s, h, r, but difficult to predict.

Cryptanalysis of Substitution Cipher: Frequency Table

Look at di-grams:

$$TH, HE, IN, ER, AN, RE, ED, ON, ES, ST,$$
$$EN, AT, TO, NT, HA, ND, OU, EA, NG, AS,$$
$$OR, TI, IS, ET, IT, AR, TE, SE, HI, OF.$$

Cryptanalysis of Substitution Cipher: Frequency Table

Look at di-grams:

$$TH, HE, IN, ER, AN, RE, ED, ON, ES, ST,$$
$$EN, AT, TO, NT, HA, ND, OU, EA, NG, AS,$$
$$OR, TI, IS, ET, IT, AR, TE, SE, HI, OF.$$

Also look at tri-grams:

$$THE, ING, AND, HER, ERE, ENT,$$
$$THA, NTH, WAS, ETH, FOR, DTH.$$

Cryptanalysis of Substitution Cipher: Frequency of Occurances

```
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$
- C, D, F, J, M, R, Y might be encryptions of t, a, o, i, n, s, h, r, but difficult to predict.

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$
- C, D, F, J, M, R, Y might be encryptions of t, a, o, i, n, s, h, r, but difficult to predict.
- Look at digrams of the form $\_Z$ and $Z\_$.

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$
- C, D, F, J, M, R, Y might be encryptions of t, a, o, i, n, s, h, r, but difficult to predict.
- Look at digrams of the form $\_Z$ and $Z\_$.
- $ZW : 4$, $WZ : 0$, W less frequent: $d_K(W) = d$

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$
- C, D, F, J, M, R, Y might be encryptions of t, a, o, i, n, s, h, r, but difficult to predict.
- Look at digrams of the form $\_Z$ and $Z\_$.
- $ZW : 4$, $WZ : 0$, W less frequent: $d_K(W) = d$
- $DZ : 4$, $ZD : 2$: $d_K(D) \in \{r, s, t\}$

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$
- C, D, F, J, M, R, Y might be encryptions of t, a, o, i, n, s, h, r, but difficult to predict.
- Look at digrams of the form $\_Z$ and $Z\_$.
- $ZW : 4$, $WZ : 0$, W less frequent: $d_K(W) = d$
- $DZ : 4$, $ZD : 2$: $d_K(D) \in \{r, s, t\}$
- $ZRW : 1$, $RW : 2$, R frequent: $d_K(R) = n$

Cryptanalysis of Substitution Cipher

```
------end---------e----ned---e-----------
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ

--------e----e---------n--d---en----e----e
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ

-e---n------n------ed---e---e--ne-nd-e-e--
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ

-ed-----n-----------e----ed-------d---e--n
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Cryptanalysis of Substitution Cipher

```
o-r-riend-ro--arise-a-inedhise--t---ass-it
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ

hs-r-riseasi-e-a-orationhadta-en--ace-hi-e
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ

he-asnt-oo-in-i-o-redso-e-ore-ineandhesett
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ

-ed-ac-inhischair-aceti-ted--to-ardsthes-n
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Cryptanalysis of Substitution Cipher

Our friend from Paris examined his empty glass with surprise, as if evaporation had taken place while he wasn't looking. I poured some more wine and he settled back in his chair, face tilted up towards the sun.[1]

Vigenere Cipher

$\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}^m$.

- Keygen: $K \leftarrow_\$ \mathbb{Z}_{26}^m$.
- Encryption: $C := (M + K) \mod 26$.
- Decryption: $M := (C + K) \mod 26$.

Poly-Alphabetic Cipher

Cryptanalysis of Vigenere Cipher

```
CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE
```

Cryptanalysis of Vigenere Cipher

- Given m, how can you decrypt?

Cryptanalysis of Vigenere Cipher

- Given m, how can you decrypt?

Can you use the following result?

- Index of coincidence: $IC = \Sigma_{i=1}^{n} \frac{f_i^2}{2^n}$, f_i freq of i-th letter.
- For a set of 26 random elements, $IC = \frac{1}{26} = 0.038$
- However, for English dictionary $IC = 0.065$

Cryptanalysis of Vigenere Cipher

- For the given ciphertext let $q_1, \ldots, q_{26}$ be the freq of i-th letter.
- Calculate $I_j = \Sigma_{i=1}^{26} p_i q_{i+j}$, for $j = 0, \ldots, 25$.
- Find k for which I_k is close to 0.065 and report that as the key.

Towards Modern Cryptography

Principles of Modern Cryptography

Ad-hoc Design

Provably Secure Design

Principles of Modern Cryptography

- Formal Definition (Power and Goal of the adversary)
- Precise Assumption
- Proofs of Security

Perfect Secrecy

Eve obtains no information about plaintext:

Definition

$$\Pr[\mathsf{M} = M \mid \mathsf{C} = C] = \Pr[\mathsf{M} = M], \ \forall M \in \mathcal{M}, \ C \in \mathcal{C}.$$

Perfect Secrecy

Eve obtains no information about plaintext:

Definition

$$\Pr[\mathsf{M} = M \mid \mathsf{C} = C] = \Pr[\mathsf{M} = M],\ \forall M \in \mathcal{M},\ C \in \mathcal{C}.$$

An Alternate Definition

$$\Pr[Enc(M_0, K) = C] = \Pr[Enc(M_1, K) = C],\ \forall M_0, M_1 \in \mathcal{M},\ C \in \mathcal{C}.$$

Perfect Secrecy

Perfect Indistinguishability

- Adv chooses two messages M_0 and M_1 of same length
- Challenger chooses b and returns $c = Enc(M_b, K)$
- Adv returns b'

Perfect Indistinguishability

- Adv chooses two messages M_0 and M_1 of same length
- Challenger chooses b and returns $c = Enc(M_b, K)$
- Adv returns b' (Goal: guess b)
- Adversary wins if it can guess b'.

Perfect Indistinguishability

- Adv chooses two messages M_0 and M_1 of same length
- Challenger chooses b and returns $c = Enc(M_b, K)$
- Adv returns b' (Goal: guess b)
- Adversary wins if it can guess b'.

Perfect Indistinguishable $\Rightarrow$ Pr[Adv wins] $= 1/2$.

Perfect Indistinguishability

- Adv chooses two messages M_0 and M_1 of same length
- Challenger chooses b and returns $c = Enc(M_b, K)$
- Adv returns b' (Goal: guess b)
- Adversary wins if it can guess b'.

Perfect Indistinguishable $\Rightarrow$ Pr[Adv wins] $= 1/2$.

Theorem

Π achieves Perfect Secrecy $\Leftrightarrow$ Π is Perfectly Indistinguishable

Perfect Secrecy: Existence

One Time Pad

$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^{\ell}$

$$Enc_K(M) = M \oplus K.$$

Perfect Secrecy: Existence

One Time Pad

$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^{\ell}$

$$Enc_K(M) = M \oplus K.$$

Perfect Secrecy

Theorem

If $\Pi :=$(KeyGen, Encryption, Decryption) is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Perfect Secrecy

Theorem

If Π :=(KeyGen, Encryption, Decryption) is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof Sketch

- $\mathcal{M}_C = \{M : Dec_K(C) = M, \text{ for some } K.\}$

Perfect Secrecy

Theorem

If $\Pi :=$(KeyGen, Encryption, Decryption) is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof Sketch

- $\mathcal{M}_C = \{M : Dec_K(C) = M, \text{ for some } K.\}$
- $|\mathcal{M}_C| \leq |\mathcal{K}|$

Perfect Secrecy

Theorem

If Π :=(KeyGen, Encryption, Decryption) is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof Sketch

- $\mathcal{M}_C = \{M : Dec_K(C) = M, \text{ for some } K.\}$
- $|\mathcal{M}_C| \leq |\mathcal{K}|$
- If $|\mathcal{K}| < |\mathcal{M}|$, there exists some M' such that $M' \in \mathcal{M}$, but $M' \notin \mathcal{M}(\mathcal{C})$ - Violates Perfect Security..!!

Perfect Secrecy

Theorem

If $\Pi :=$(KeyGen, Encryption, Decryption) is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Computational Security

Perfect Security is too strong

- Absolutely no information about an encrypted message is leaked.
- Moreover, the adversary has unlimited computational power.

Computational Security

Perfect Security is too strong

- Absolutely no information about an encrypted message is leaked.
- Moreover, the adversary has unlimited computational power.

How about a scheme that leaks information with

- probability at most 2^{-60} to adversaries
- investing up to 200 years of computational effort on the fastest available supercomputer?

Computational Security

A scheme is (t, ϵ)-secure if any adversary

- running for time at most t
- succeeds in breaking the scheme with probability at most ϵ.

Computational Indistinguishability

- Adv chooses two messages M_0 and M_1 of same length
- Challenger chooses b and returns $c = Enc(M_b, K)$
- Adv returns b'

Computational Indistinguishability

- Adv chooses two messages M_0 and M_1 of same length
- Challenger chooses b and returns $c = Enc(M_b, K)$
- Adv returns b' (Goal: guess b)
- Adversary wins if it can guess b'.

Computational Indistinguishability

- Adv chooses two messages M_0 and M_1 of same length
- Challenger chooses b and returns $c = Enc(M_b, K)$
- Adv returns b' (Goal: guess b)
- Adversary wins if it can guess b'.

Computationally Indistinguishable $\Rightarrow$ Pr[Adv wins] $= 1/2 + \epsilon$.

Computational Indistinguishability

- Adv chooses two messages M_0 and M_1 of same length
- Challenger chooses b and returns $c = Enc(M_b, K)$
- Adv returns b' (Goal: guess b)
- Adversary wins if it can guess b'.

Computationally Indistinguishable $\Rightarrow$ Pr[Adv wins] $= 1/2 + \epsilon$.

IND-CPA Security

Adv is given the power to make encryption queries except M_0 and M_1.

Designing A Provably Secure Encryption Construction

- Formal Definition (✓)

Designing A Provably Secure Encryption Construction

- Formal Definition (✓)
- Precise Assumptions
  - Notions of Pseudo-Random Generator (PRG), Pseudo-Random Function (PRF)
  - Assume such function exists

Designing A Provably Secure Encryption Construction

- Formal Definition (✓)
- Precise Assumptions
  - Notions of Pseudo-Random Generator (PRG), Pseudo-Random Function (PRF)
  - Assume such function exists
- Proofs of Security
  - Encryption Scheme based on PRG G and PRF F.
  - Reduction-based Proofs.

References

- Introduction to Modern Cryptography by *Jonathan Katz* and *Yehuda Lindell* (✓)
- Cryptography - Theory and Practice by *Douglas Stinson*
- A Graduate Course in Applied Cryptography by *Dan Boneh* and *Victor Shoup*

Thank You..!!!