Testing LaTeX sty file

Lecturer(s): ChatGPT

Author: Saurav Banka

Semester: HS 2025

Last edited: September 22, 2025

Contents

1 Testing Colored Boxes

1.1 What are those

Theorem 1.1. Every odd number is the difference of two squares.

Lemma 1.1. If p divides ab, then p divides a or b.

Definition 1.1. A prime is a number with no nontrivial divisors.

Example 1.1. The number 7 is prime.

Exercise 1.1. Prove that there are infinitely many primes.

1.2 What are these

Note 1.1. This is equivalent to showing that primes cannot be bounded above.

Theorem 1.2. If something is suspicious...

Proof. Let n be odd. Then $n = 2k + 1$. Observe that

$$(k+1)^2 - (k)^2 = (k^2 + 2k + 1) - k^2 = 2k + 1 = n.$$

Thus every odd number is a difference of two squares. □

Proposition 1.1 (Bayes Rule). $\Pr(A \mid B) = \dfrac{\Pr(B \mid A)\Pr(A)}{\Pr(B)}$.

Corollary 1.1. Every prime p is either 2 or odd.....

2 Math Shorthands

Some math macros and operators:

2.1 Probability

$$X \sim \mathrm{Bin}(n, p), \quad Y \sim \mathrm{Ber}(\theta), \quad Z \sim \mathcal{N}(0, 1).$$
$$\theta \sim \mathrm{Beta}(\alpha, \beta), \quad \lambda \sim \mathrm{Gamma}(k, \theta), \quad N \sim \mathrm{Delta}(\mu).$$
$$\mathbb{E}[X], \quad \mathrm{Var}(X), \quad \mathrm{Cov}(X, Y), \quad \Pr(A \cap B).$$

Conditional expectation: $\mathbb{E}\left[X \,|\, Y\right]$
Conditional probability: $\mathbb{P}\left(A \,|\, B\right)$
Density notation: $p(x)\,, q(z)$

2.1.1 Gaussian Processes

Define prior: $f \sim \mathcal{GP}(0, k(x, x'))$
Posterior mean: $\mu'(x^*) = k(x^*, X)\left(\mathbf{K} + \sigma^2 I\right)^{-1} y$

2.2 Optimization

$$\arg\min_{x \in \mathbb{R}^n} f(x), \qquad \arg\max_{\theta \in \Theta} \Pr(D \mid \theta).$$
$$\sup_{x \in \mathbb{R}} g(x), \qquad \inf_{n \geq 1} a_n.$$

2.3 Linear Algebra

$$A\boldsymbol{v} = \lambda \boldsymbol{v}, \quad \mathrm{rank}(A), \quad \mathrm{tr}(A), \quad \mathrm{Null}(A).$$

Transpose: A^{T}
Inverse: A^{-1}
Half fraction: $\frac{1}{2}x^2$
Diagonal matrix: $\mathrm{diag}(\boldsymbol{x})$

3 Warnings and Drafts


This section might contain misleading or incomplete arguments.


Do not attempt this at home: Probability measure $\mathbb{P}$ over an uncountable set can behave counterintuitively.

DRAFT — September 22, 2025

Algorithm 1 Sample Pseudocode

Initialize $x \leftarrow 0$
while $x < 10$ **do**
    $x \leftarrow x + 1$
return x

4 Algorithms

5 Cross References

We can reference earlier results:

- See Theorem 1.1.
- See Lemma 1.1.
- See Definition 1.1.
- See Example 1.1.
- See Exercise 1.1.

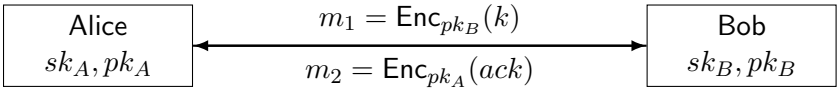
6 Cryptography Examples

6.1 Notation

An encryption scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CPA-secure if for all PPT adversaries $\mathcal{A}$,

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}CPA}}(\lambda) \leq \mathsf{negl}(\lambda).$$

6.2 Protocol Diagram

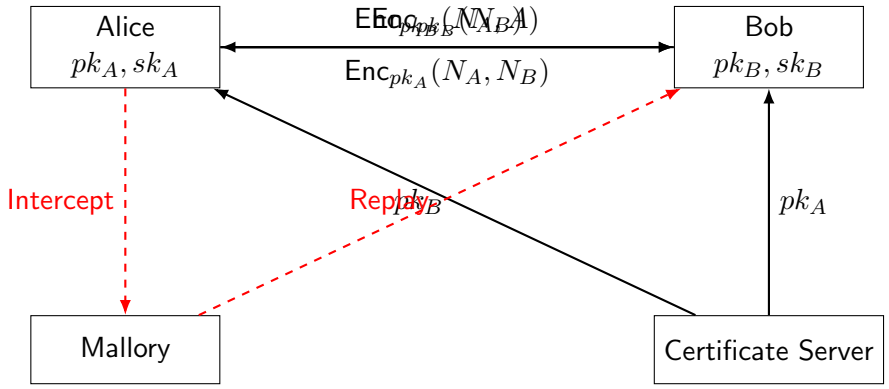


6.3 Crypto Algorithm

Algorithm 2 Key Exchange (simplified)

Input: Security parameter λ
$A, B \leftarrow \mathsf{KeyGen}(1^\lambda)$
chooserandom $k \in \{0,1\}^\lambda$
$c \leftarrow \mathsf{Enc}_{pk_B}(k)$
Send c to Bob
Bob: $k' \leftarrow \mathsf{Dec}_{sk_B}(c)$
returnshared key k

6.4 Needham–Schroeder Protocol Example



6.5 Alice's Steps

Algorithm 3 Alice (Needham–Schroeder Initiator)

Input: pk_B from Certificate Server
choosefresh nonce N_A
$c_1 \leftarrow \mathsf{Enc}_{pk_B}(N_A, A)$
Send c_1 to Bob
Receive c_2
$(N'_A, N_B) \leftarrow \mathsf{Dec}_{sk_A}(c_2)$
if $N'_A = N_A$ **then**
    $c_3 \leftarrow \mathsf{Enc}_{pk_B}(N_B)$
    Send c_3 to Bob
    returnsuccess
else
    returnabort

6.6 Bob's Steps

7 Draft notes and side notes

This is a sentence. ¡¡Check this step later.¿¿
This needs a picture . Draw diagram here

Algorithm 4 Bob (Needham–Schroeder Responder)

Input: pk_A from Certificate Server
Receive c_1
$(N_A, A) \leftarrow \mathsf{Dec}_{sk_B}(c_1)$
choosefresh nonce N_B
$c_2 \leftarrow \mathsf{Enc}_{pk_A}(N_A, N_B)$
Send c_2 to Alice
Receive c_3
$N'_B \leftarrow \mathsf{Dec}_{sk_B}(c_3)$
if $N'_B = N_B$ **then**
    returnauthenticated session
else
    returnabort

A Background on Measure Theory

Appendix material here.

B Background on Information Theory

No information....

C Bibliography Example

We can cite classic references: see [2, 1].

References

[1] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley, 2006.

[2] Walter Rudin. *Real and Complex Analysis*. McGraw-Hill, 1987.