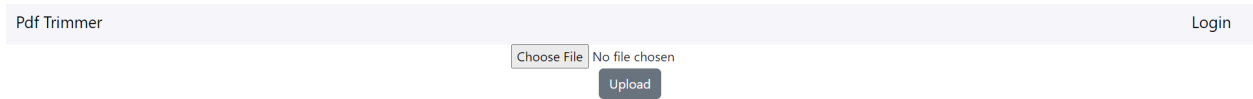
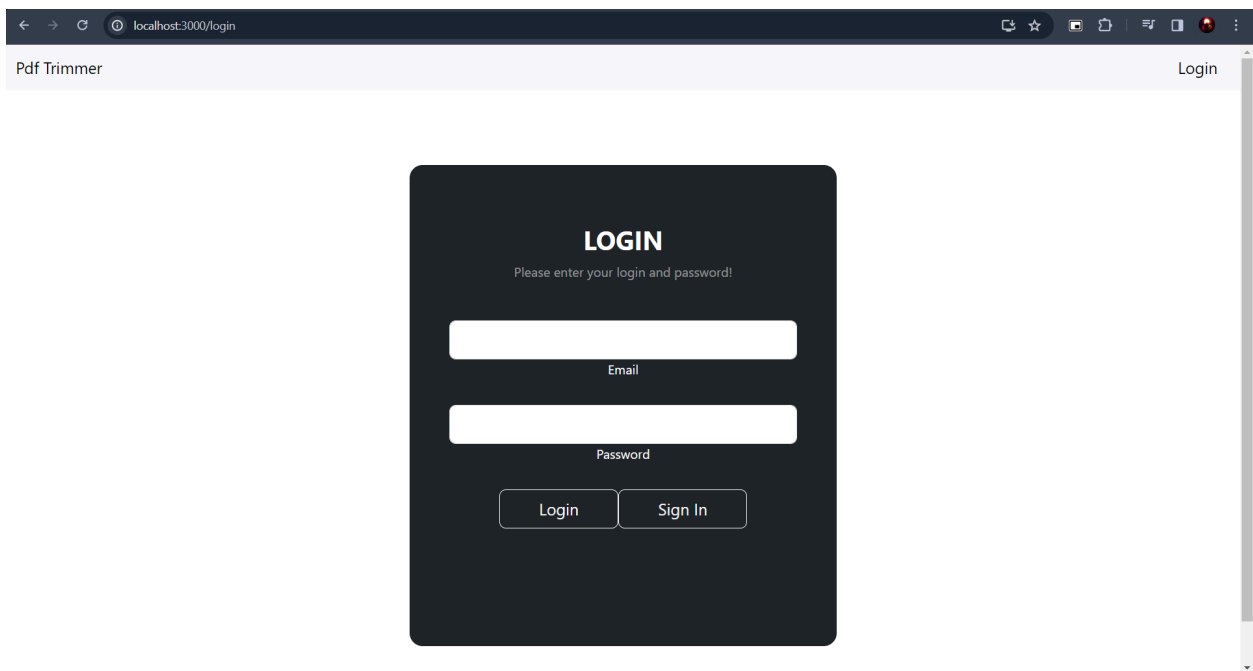


# ScreenShots ( various scenarios )

## Initial page



## Login Page



## Selecting pages after uploading pdf

Pdf Trimmer

user@gmail.com

Choose File

RSA\_Attacks.pdf

Upload

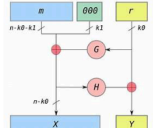
Checkbox 4

Optimum Asymmetric Encryption Padding

Let  $n$  is the number of bits of the modulus. We always select messages  $m$  of  $n - k_0 - k_1$  bits.

$G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k_1}$  is a one-way mapping.

$H : \{0, 1\}^{n-k_0} \rightarrow \{0, 1\}^{k_1}$  is a one-way function.



Checkbox 5

Wiener's Small Decryption Exponent Attack

**Wiener's Statement**  
If the decryption exponent is Low i.e.  $3d \leq N^{\frac{1}{4}}$ , then it is easy to determine the private exponent ( $d$ ) with the public information ( $e, N$ ).  
We assume that the factors of  $N$  (i.e.  $q, p$ ) are equal in size.

The attack works when  $d$  has fewer than  
 $\ell/4 - 1$  bits, where  $\ell = \log_2 N$  the size of  $N$

Page 1

Page 2

Page 4

Page 5

## After Downloading

Choose File

RSA\_Attacks.pdf

Upload

Show pdf

Download

3db29d5d-37f2-4eec-93d3-1277c1b8c010.pdf

51.5 KB • Done

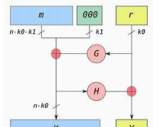
Checkbox 4

Optimum Asymmetric Encryption Padding

Let  $n$  is the number of bits of the modulus. We always select messages  $m$  of  $n - k_0 - k_1$  bits.

$G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k_1}$  is a one-way mapping.

$H : \{0, 1\}^{n-k_0} \rightarrow \{0, 1\}^{k_1}$  is a one-way function.



Checkbox 5

Wiener's Small Decryption Exponent Attack

**Wiener's Statement**  
If the decryption exponent is Low i.e.  $3d \leq N^{\frac{1}{4}}$ , then it is easy to determine the private exponent ( $d$ ) with the public information ( $e, N$ ).  
We assume that the factors of  $N$  (i.e.  $q, p$ ) are equal in size.

The attack works when  $d$  has fewer than  
 $\ell/4 - 1$  bits, where  $\ell = \log_2 N$  the size of  $N$

Page 3

Page 4

Page 5