Modern Cryptography

Project 2 : Blog Application

Prof. Giovanni Di Crescenzo

Rajat Pawar (N13295898)
Jay Patel (N10541249)

Introduction

- Blog Application

1. User registration
2. Post blog
3. View blog

Idea Of Security

- Completely secure system is a virtual impossibility.
- An approach often used in the security profession is one of balancing risk and usability

Possible Threats To Application

- Data modification
  - Data can be changed in between communication channel
  - Man in the middle
- Data replay
  - Attacker can resend the same request which was captured previously
- Data eavesdropping
  - Attacker can sniff the traffic between client and server.
- Data storage
  - How data is stored on the server?
- Key management
  - How keys are stored?

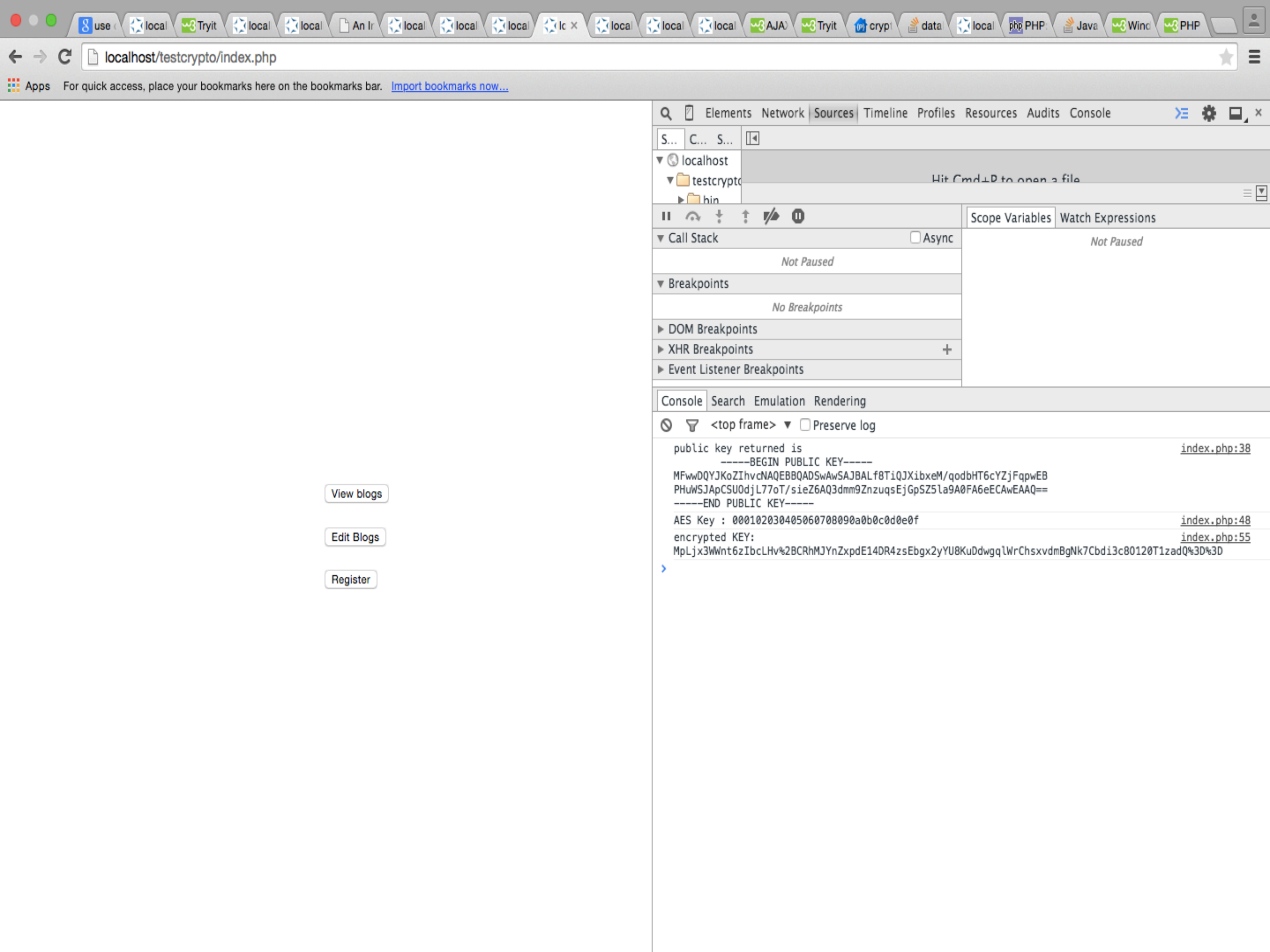
Cryptographic Steps

- Used HTML5 secure local storage in browser to store the client side keys.
- Implemented Asymmetric key algorithm to encrypt the communication between client and server.
- Used session variables to mitigate the data replay attacks.
- Implemented native methods to store data securely on server.

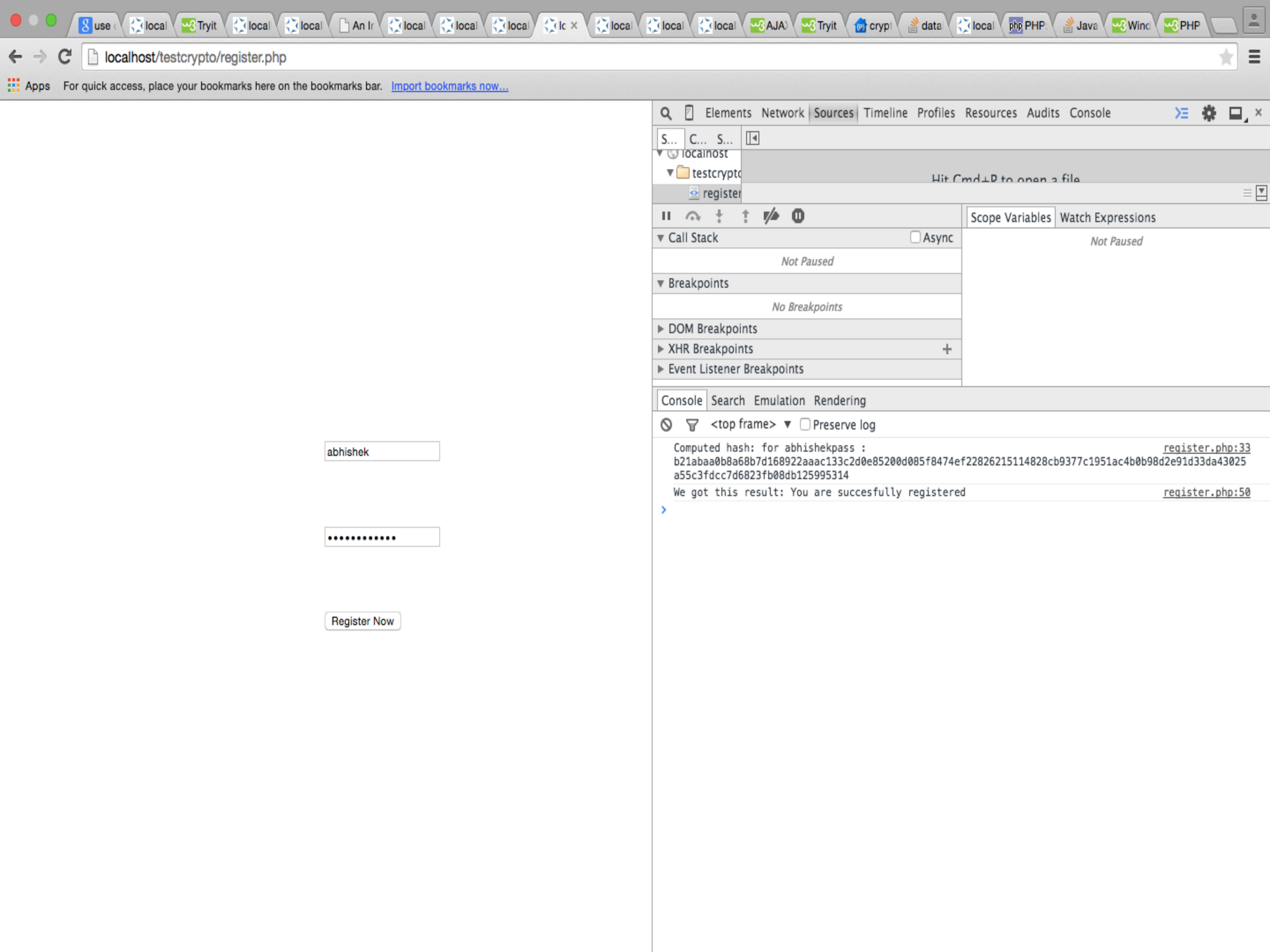
Implementation

- Server side:
  - php
  - C++
  - Openssl
- Client side:
  - HTML5
  - Javascript
  - AJAX
  - crytoJS

Screenshots



```
public key returned is                                                        index.php:38
        -----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALf8TiQJXibxeM/qodbHT6cYZjFqpwEB
PHuWSJApCSUOdjL77oT/sieZ6AQ3dmm9ZnzuqsEjGpSZ5la9A0FA6eECAwEAAQ==
-----END PUBLIC KEY-----
AES Key : 000102030405060708090a0b0c0d0e0f                                    index.php:48
encrypted KEY:                                                                index.php:55
MpLjx3WWnt6zIbcLHv%2BCRhMJYnZxpdE14DR4zsEbgx2yYU8KuDdwgqlWrChsxvdmBgNk7Cbdi3c80120T1zadQ%3D%3D
```



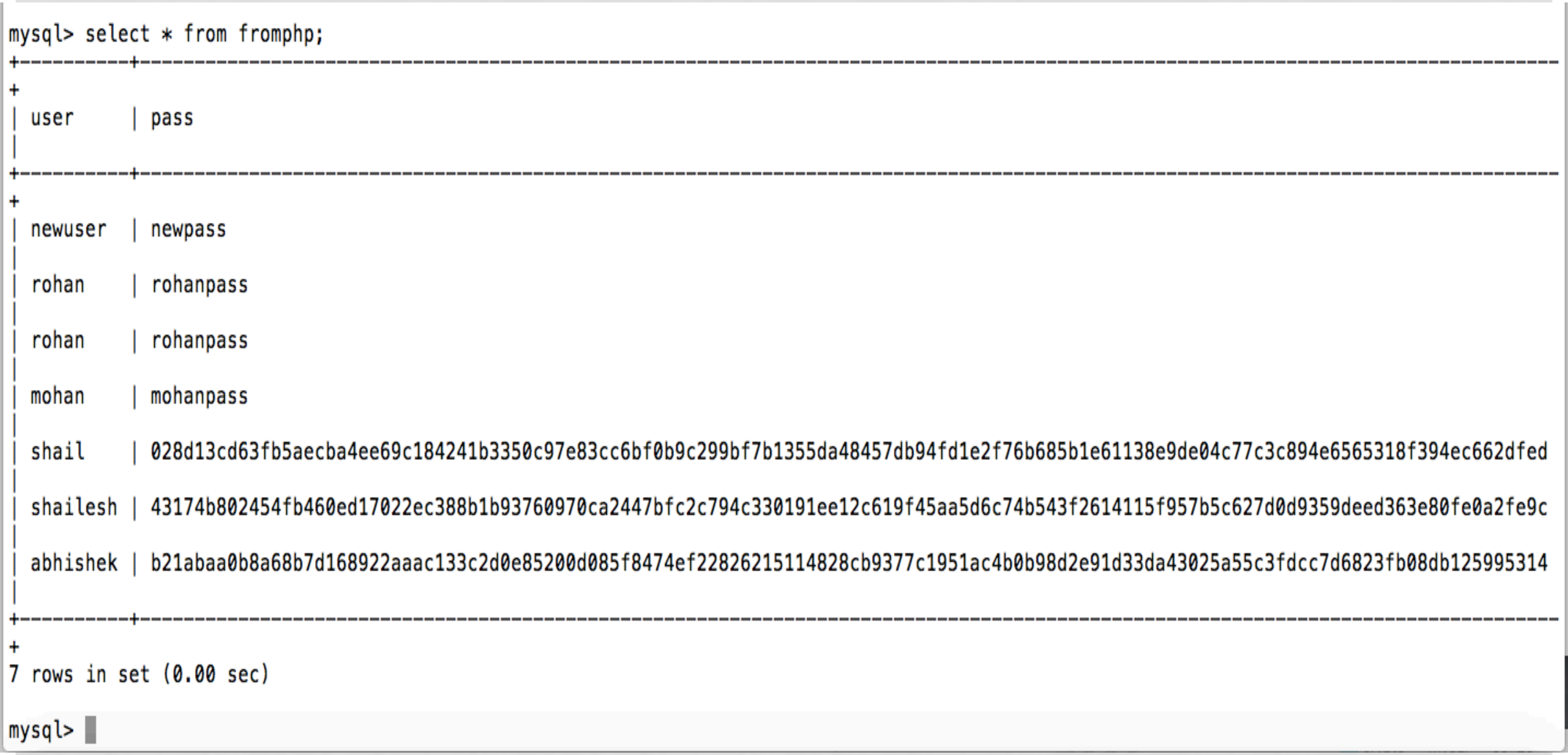
localhost/testcrypto/register.php

abhishek

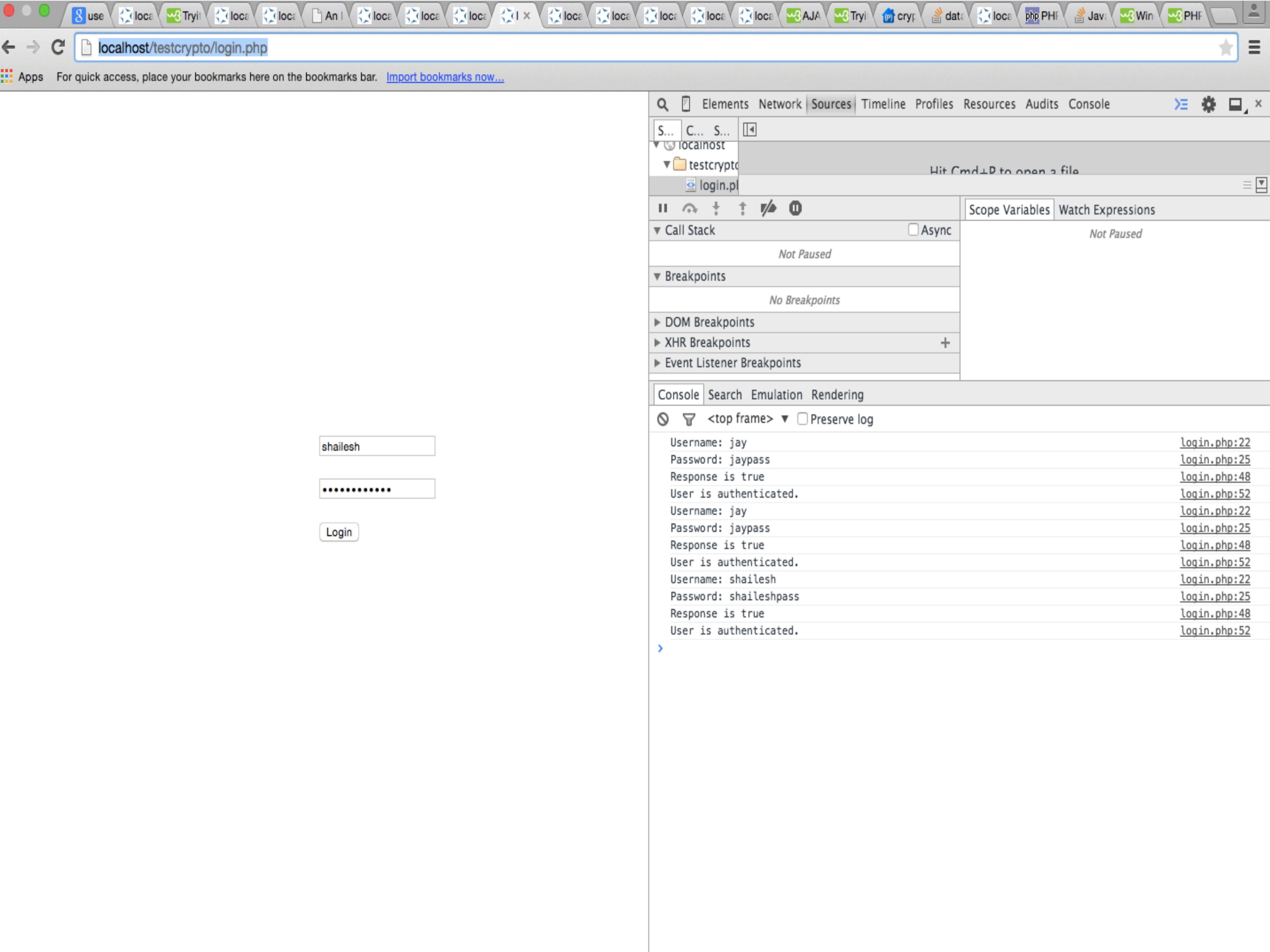
•••••••••••••

Register Now

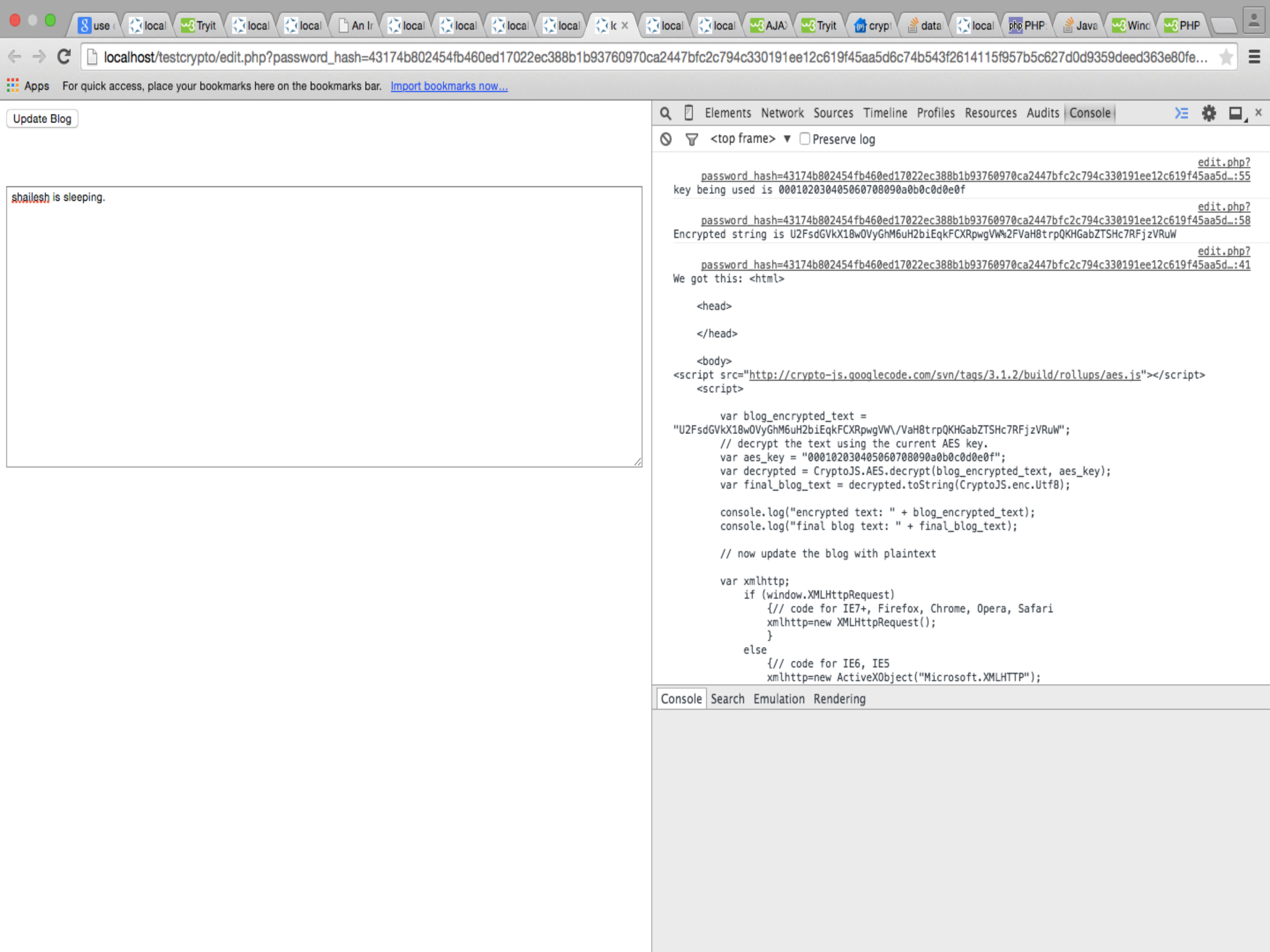
```
Computed hash: for abhishekpass :                                                    register.php:33
b21abaa0b8a68b7d168922aaac133c2d0e85200d085f8474ef22826215114828cb9377c1951ac4b0b98d2e91d33da43025
a55c3fdcc7d6823fb08db125995314
We got this result: You are succesfully registered                                   register.php:50
```



```
mysql> select * from fromphp;
+----------+----------------------------------------------------------------------------------------------------------------------------------
+
| user     | pass
|
+----------+----------------------------------------------------------------------------------------------------------------------------------
+
| newuser  | newpass
|
| rohan    | rohanpass
|
| rohan    | rohanpass
|
| mohan    | mohanpass
|
| shail    | 028d13cd63fb5aecba4ee69c184241b3350c97e83cc6bf0b9c299bf7b1355da48457db94fd1e2f76b685b1e61138e9de04c77c3c894e6565318f394ec662dfed
|
| shailesh | 43174b802454fb460ed17022ec388b1b93760970ca2447bfc2c794c330191ee12c619f45aa5d6c74b543f2614115f957b5c627d0d9359deed363e80fe0a2fe9c
|
| abhishek | b21abaa0b8a68b7d168922aaac133c2d0e85200d085f8474ef22826215114828cb9377c1951ac4b0b98d2e91d33da43025a55c3fdcc7d6823fb08db125995314
|
+----------+----------------------------------------------------------------------------------------------------------------------------------
+
7 rows in set (0.00 sec)

mysql> 
```

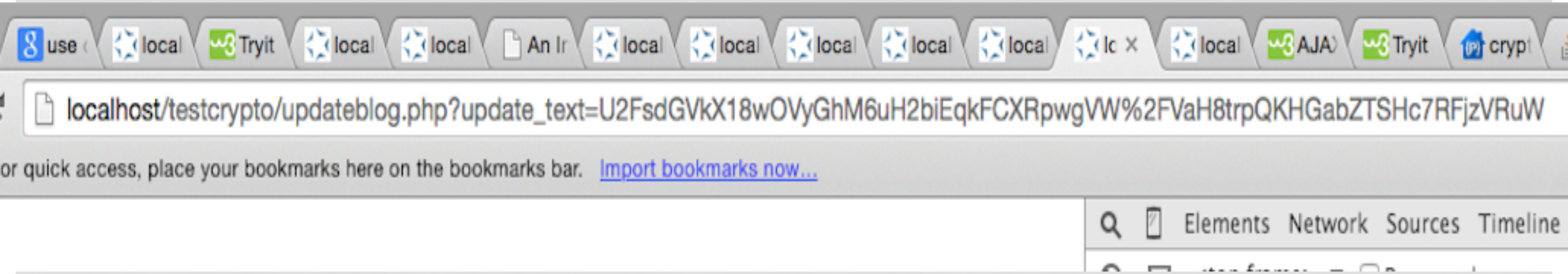


```
Username: jay                          login.php:22
Password: jaypass                      login.php:25
Response is true                       login.php:48
User is authenticated.                 login.php:52
Username: jay                          login.php:22
Password: jaypass                      login.php:25
Response is true                       login.php:48
User is authenticated.                 login.php:52
Username: shailesh                     login.php:22
Password: shaileshpass                 login.php:25
Response is true                       login.php:48
User is authenticated.                 login.php:52
```


localhost/testcrypto/edit.php?password_hash=43174b802454fb460ed17022ec388b1b93760970ca2447bfc2c794c330191ee12c619f45aa5d6c74b543f2614115f957b5c627d0d9359deed363e80fe...
Apps
For quick access, place your bookmarks here on the bookmarks bar.
Import bookmarks now...
Update Blog
Elements
Network
Sources
Timeline
Profiles
Resources
Audits
Console
<top frame>
Preserve log
Console
Search
Emulation
Rendering

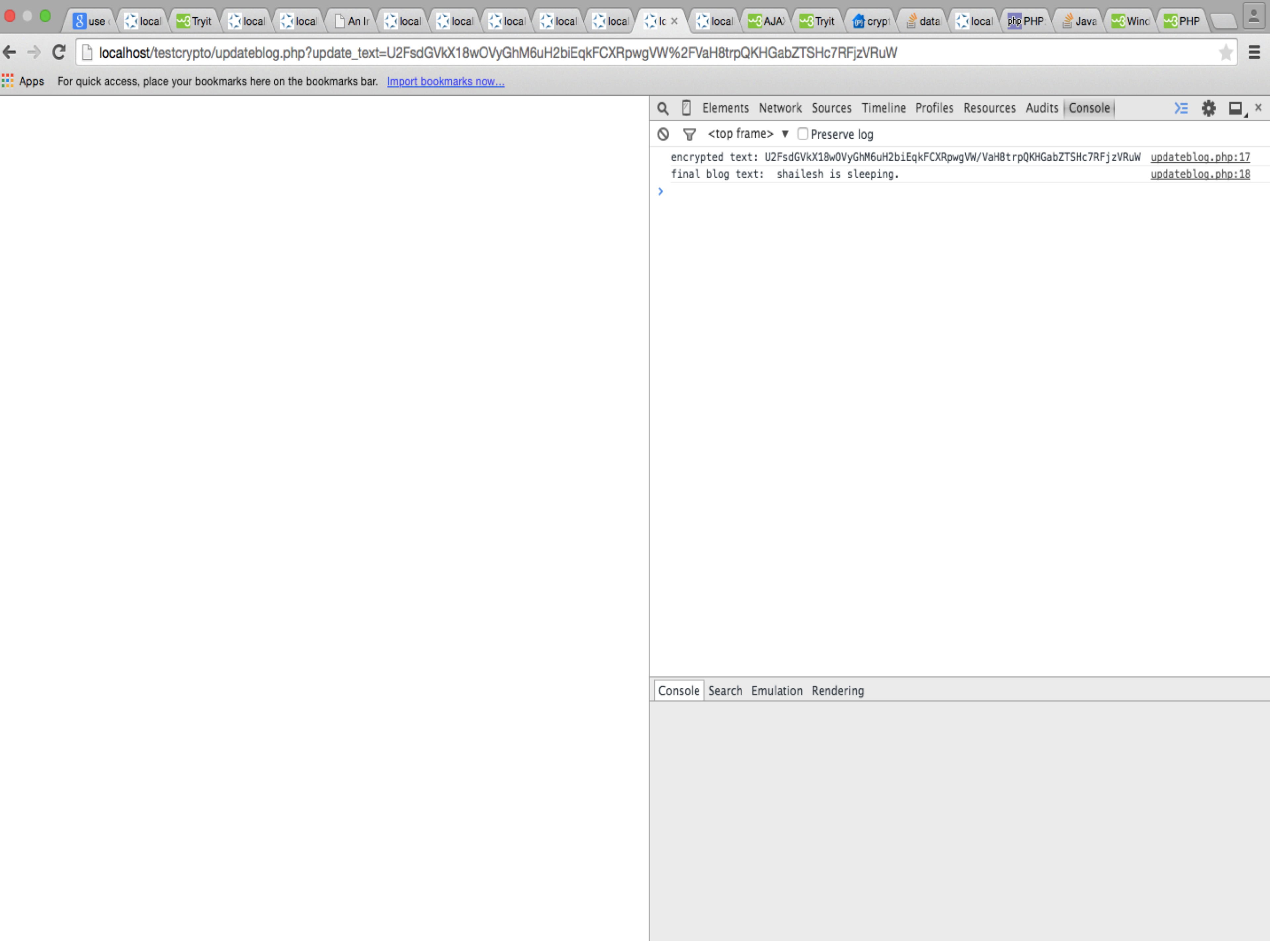
shailesh is sleeping.

```
                                                                                     edit.php?
    password_hash=43174b802454fb460ed17022ec388b1b93760970ca2447bfc2c794c330191ee12c619f45aa5d…:55
key being used is 000102030405060708090a0b0c0d0e0f
                                                                                     edit.php?
    password_hash=43174b802454fb460ed17022ec388b1b93760970ca2447bfc2c794c330191ee12c619f45aa5d…:58
Encrypted string is U2FsdGVkX18wOVyGhM6uH2biEqkFCXRpwgVW%2FVaH8trpQKHGabZTSHc7RFjzVRuW
                                                                                     edit.php?
    password_hash=43174b802454fb460ed17022ec388b1b93760970ca2447bfc2c794c330191ee12c619f45aa5d…:41
We got this: <html>

    <head>

    </head>

    <body>
<script src="http://crypto-js.googlecode.com/svn/tags/3.1.2/build/rollups/aes.js"></script>
    <script>

        var blog_encrypted_text =
"U2FsdGVkX18wOVyGhM6uH2biEqkFCXRpwgVW\/VaH8trpQKHGabZTSHc7RFjzVRuW";
        // decrypt the text using the current AES key.
        var aes_key = "000102030405060708090a0b0c0d0e0f";
        var decrypted = CryptoJS.AES.decrypt(blog_encrypted_text, aes_key);
        var final_blog_text = decrypted.toString(CryptoJS.enc.Utf8);

        console.log("encrypted text: " + blog_encrypted_text);
        console.log("final blog text: " + final_blog_text);

        // now update the blog with plaintext

        var xmlhttp;
            if (window.XMLHttpRequest)
                {// code for IE7+, Firefox, Chrome, Opera, Safari
                xmlhttp=new XMLHttpRequest();
                }
            else
                {// code for IE6, IE5
                xmlhttp=new ActiveXObject("Microsoft.XMLHTTP");
```



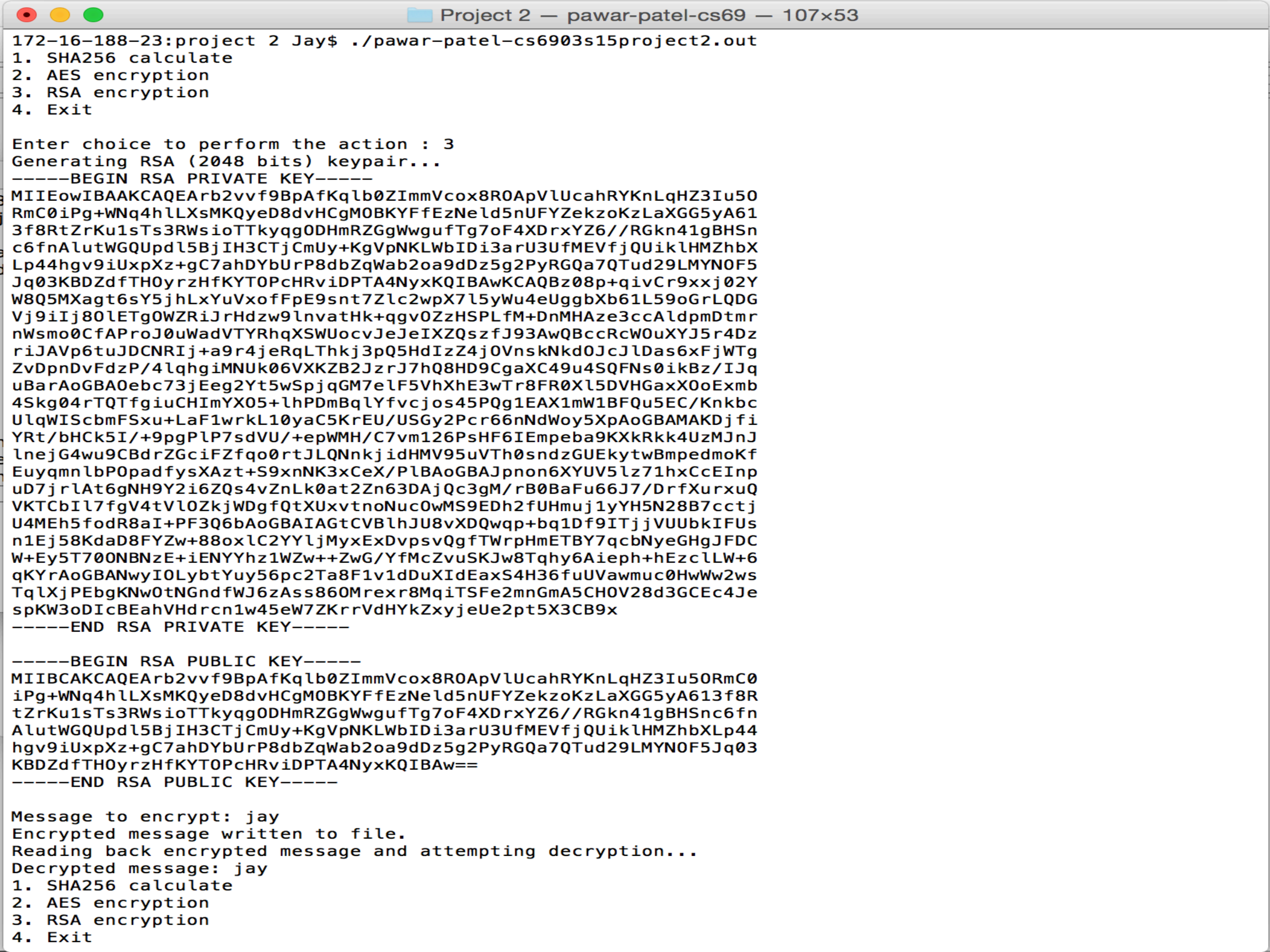
localhost/testcrypto/updateblog.php?update_text=U2FsdGVkX18wOVyGhM6uH2biEqkFCXRpwgVW%2FVaH8trpQKHGabZTSHc7RFjzVRuW

or quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

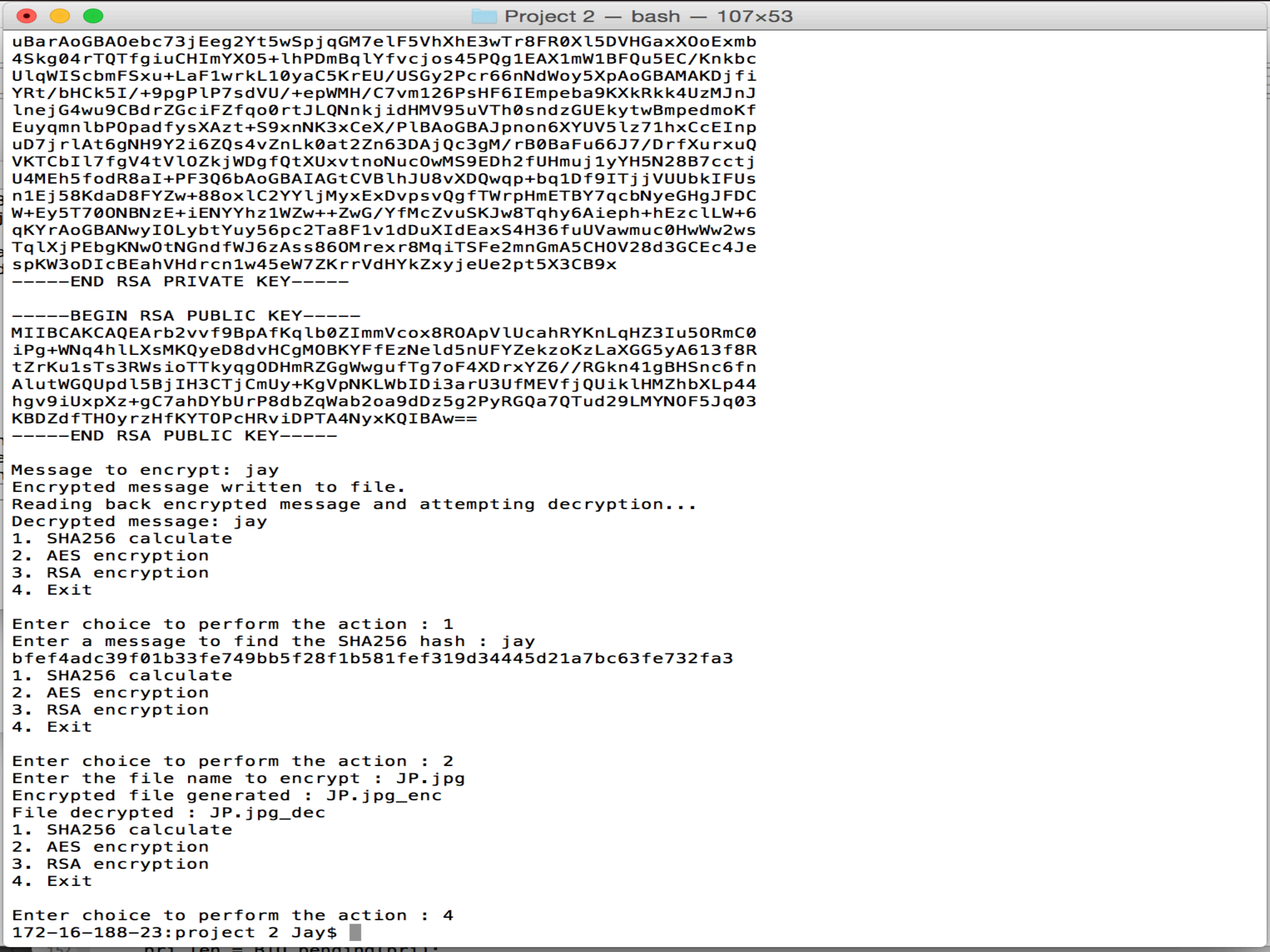


```
localhost/testcrypto/updateblog.php?update_text=U2FsdGVkX18wOVyGhM6uH2biEqkFCXRpwgVW%2FVaH8trpQKHGabZTSHc7RFjzVRuW
```

```
encrypted text: U2FsdGVkX18wOVyGhM6uH2biEqkFCXRpwgVW/VaH8trpQKHGabZTSHc7RFjzVRuW  updateblog.php:17
final blog text:  shailesh is sleeping.                                           updateblog.php:18
>
```



```
172-16-188-23:project 2 Jay$ ./pawar-patel-cs6903s15project2.out
1. SHA256 calculate
2. AES encryption
3. RSA encryption
4. Exit

Enter choice to perform the action : 3
Generating RSA (2048 bits) keypair...
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEArb2vvf9BpAfKqlb0ZImmVcox8ROApVlUcahRYKnLqHZ3Iu5O
RmC0iPg+WNq4hlLXsMKQyeD8dvHCgMOBKYFfEzNeld5nUFYZekzoKzLaXGG5yA61
3f8RtZrKu1sTs3RWsioTTkyqgODHmRZGgWwgufTg7oF4XDrxYZ6//RGkn41gBHSn
c6fnAlutWGQUpdl5BjIH3CTjCmUy+KgVpNKLWbIDi3arU3UfMEVfjQUiklHMZhbX
Lp44hgv9iUxpXz+gC7ahDYbUrP8dbZqWab2oa9dDz5g2PyRGQa7QTud29LMYNOF5
Jq03KBDZdfTHOyrzHfKYTOPcHRviDPTA4NyxKQIBAwKCAQBz08p+qivCr9xxj02Y
W8Q5MXagt6sY5jhLxYuVxofFpE9snt7Zlc2wpX7l5yWu4eUggbXb61L59oGrLQDG
Vj9iIj8OlETgOWZRiJrHdzw9lnvatHk+qgvOZzHSPLfM+DnMHAze3ccAldpmDtmr
nWsmo0CfAProJ0uWadVTYRhqXSWUocvJeJeIXZQszfJ93AwQBccRcWOuXYJ5r4Dz
riJAVp6tuJDCNRIj+a9r4jeRqLThkj3pQ5HdIzZ4jOVnskNkdOJcJlDas6xFjWTg
ZvDpnDvFdzP/4lqhgiMNUk06VXKZB2JzrJ7hQ8HD9CgaXC49u4SQFNs0ikBz/IJq
uBarAoGBAOebc73jEeg2Yt5wSpjqGM7elF5VhXhE3wTr8FR0Xl5DVHGaxXOoExmb
4Skg04rTQTfgiuCHImYXO5+lhPDmBqlYfvcjos45PQg1EAX1mW1BFQu5EC/Knkbc
UlqWIScbmFSxu+LaF1wrkL10yaC5KrEU/USGy2Pcr66nNdWoy5XpAoGBAMAKDjfi
YRt/bHCk5I/+9pgPlP7sdVU/+epWMH/C7vm126PsHF6IEmpeba9KXkRkk4UzMJnJ
lnejG4wu9CBdrZGciFZfqo0rtJLQNnkjidHMV95uVTh0sndzGUEkytwBmpedmoKf
EuyqmnlbPOpadfysXAzt+S9xnNK3xCeX/PlBAoGBAJpnon6XYUV5lz71hxCcEInp
uD7jrlAt6gNH9Y2i6ZQs4vZnLk0at2Zn63DAjQc3gM/rB0BaFu66J7/DrfXurxuQ
VKTCbIl7fgV4tVlOZkjWDgfQtXUxvtnoNucOwMS9EDh2fUHmuj1yYH5N28B7cctj
U4MEh5fodR8aI+PF3Q6bAoGBAIAGtCVBlhJU8vXDQwqp+bq1Df9ITjjVUUbkIFUs
n1Ej58KdaD8FYZw+88oxlC2YYljMyxExDvpsvQgfTWrpHmETBY7qcbNyeGHgJFDC
W+Ey5T70ONBNzE+iENYYhz1WZw++ZwG/YfMcZvuSKJw8Tqhy6Aieph+hEzclLW+6
qKYrAoGBANwyIOLybtYuy56pc2Ta8F1v1dDuXIdEaxS4H36fuUVawmuc0HwWw2ws
TqlXjPEbgKNwOtNGndfWJ6zAss86OMrexr8MqiTSFe2mnGmA5CHOV28d3GCEc4Je
spKW3oDIcBEahVHdrcn1w45eW7ZKrrVdHYkZxyjeUe2pt5X3CB9x
-----END RSA PRIVATE KEY-----

-----BEGIN RSA PUBLIC KEY-----
MIIBCAKCAQEArb2vvf9BpAfKqlb0ZImmVcox8ROApVlUcahRYKnLqHZ3Iu5ORmC0
iPg+WNq4hlLXsMKQyeD8dvHCgMOBKYFfEzNeld5nUFYZekzoKzLaXGG5yA613f8R
tZrKu1sTs3RWsioTTkyqgODHmRZGgWwgufTg7oF4XDrxYZ6//RGkn41gBHSnc6fn
AlutWGQUpdl5BjIH3CTjCmUy+KgVpNKLWbIDi3arU3UfMEVfjQUiklHMZhbXLp44
hgv9iUxpXz+gC7ahDYbUrP8dbZqWab2oa9dDz5g2PyRGQa7QTud29LMYNOF5Jq03
KBDZdfTHOyrzHfKYTOPcHRviDPTA4NyxKQIBAw==
-----END RSA PUBLIC KEY-----

Message to encrypt: jay
Encrypted message written to file.
Reading back encrypted message and attempting decryption...
Decrypted message: jay
1. SHA256 calculate
2. AES encryption
3. RSA encryption
4. Exit
```



```
uBarAoGBAOebc73jEeg2Yt5wSpjqGM7elF5VhXhE3wTr8FR0Xl5DVHGaxXOoExmb
4Skg04rTQTfgiuCHImYXO5+lhPDmBqlYfvcjos45PQg1EAX1mW1BFQu5EC/Knkbc
UlqWIScbmFSxu+LaF1wrkL10yaC5KrEU/USGy2Pcr66nNdWoy5XpAoGBAMAKDjfi
YRt/bHCk5I/+9pgPlP7sdVU/+epWMH/C7vm126PsHF6IEmpeba9KXkRkk4UzMJnJ
lnejG4wu9CBdrZGciFZfqo0rtJLQNnkjidHMV95uVTh0sndzGUEkytwBmpedmoKf
EuyqmnlbPOpadfysXAzt+S9xnNK3xCeX/PlBAoGBAJpnon6XYUV5lz71hxCcEInp
uD7jrlAt6gNH9Y2i6ZQs4vZnLk0at2Zn63DAjQc3gM/rB0BaFu66J7/DrfXurxuQ
VKTCbIl7fgV4tVlOZkjWDgfQtXUxvtnoNucOwMS9EDh2fUHmuj1yYH5N28B7cctj
U4MEh5fodR8aI+PF3Q6bAoGBAIAGtCVBlhJU8vXDQwqp+bq1Df9ITjjVUUbkIFUs
n1Ej58KdaD8FYZw+88oxlC2YYljMyxExDvpsvQgfTWrpHmETBY7qcbNyeGHgJFDC
W+Ey5T70ONBNzE+iENYYhz1WZw++ZwG/YfMcZvuSKJw8Tqhy6Aieph+hEzclLW+6
qKYrAoGBANwyIOLybtYuy56pc2Ta8F1v1dDuXIdEaxS4H36fuUVawmuc0HwWw2ws
TqlXjPEbgKNwOtNGndfWJ6zAss86OMrexr8MqiTSFe2mnGmA5CHOV28d3GCEc4Je
spKW3oDIcBEahVHdrcn1w45eW7ZKrrVdHYkZxyjeUe2pt5X3CB9x
-----END RSA PRIVATE KEY-----

-----BEGIN RSA PUBLIC KEY-----
MIIBCAKCAQEArb2vvf9BpAfKqlb0ZImmVcox8ROApVlUcahRYKnLqHZ3Iu5ORmC0
iPg+WNq4hlLXsMKQyeD8dvHCgMOBKYFfEzNeld5nUFYZekzoKzLaXGG5yA613f8R
tZrKu1sTs3RWsioTTkyqgODHmRZGgWwgufTg7oF4XDrxYZ6//RGkn41gBHSnc6fn
AlutWGQUpdl5BjIH3CTjCmUy+KgVpNKLWbIDi3arU3UfMEVfjQUiklHMZhbXLp44
hgv9iUxpXz+gC7ahDYbUrP8dbZqWab2oa9dDz5g2PyRGQa7QTud29LMYNOF5Jq03
KBDZdfTHOyrzHfKYTOPcHRviDPTA4NyxKQIBAw==
-----END RSA PUBLIC KEY-----

Message to encrypt: jay
Encrypted message written to file.
Reading back encrypted message and attempting decryption...
Decrypted message: jay
1. SHA256 calculate
2. AES encryption
3. RSA encryption
4. Exit

Enter choice to perform the action : 1
Enter a message to find the SHA256 hash : jay
bfef4adc39f01b33fe749bb5f28f1b581fef319d34445d21a7bc63fe732fa3
1. SHA256 calculate
2. AES encryption
3. RSA encryption
4. Exit

Enter choice to perform the action : 2
Enter the file name to encrypt : JP.jpg
Encrypted file generated : JP.jpg_enc
File decrypted : JP.jpg_dec
1. SHA256 calculate
2. AES encryption
3. RSA encryption
4. Exit

Enter choice to perform the action : 4
172-16-188-23:project 2 Jay$
```

Questions??

Thank You!