ASP.NET Encryption

Lecture: http://onlinevideo.napier.ac.uk/Play.aspx?VideoId=146
Tutorial: http://buchananweb.co.uk/2011_tut_encryption.pdf

A Base-64 Encoding/Decoding

A.1. Base-64 is often used to convert from a binary format, with non-printable characters, into a format which uses readable ASCII characters. In this example we will use the standard methods of **Convert.ToBase64String()** and **Convert.FromBase64String()** to change to and from Base-64.

A.2. First **Create a New Web Site**, then **Add a New Item** … to this, and select a **Web Form**. Using this ASP.NET Web form, create the page shown in Figure 1, with three text boxes, and one button (you do not need the rest of the page, just these three elements). The Text boxes should be named **message**, **tbEncode**, and **tbDecode64**.

A.3. Next associate the following code to the button Click event:

```
string message;
message = this.message.Text;

 this.tbEncode.Text = base64Encode(message);
 this.tbDecode64.Text = base64Decode(this.tbEncode.Text);
```

A.4. Finally, add two methods of:

```
public string base64Decode(string data)
 {
 // Based on: http://www.vbforums.com/showthread.php?s=&threadid=287324
try
{
 System.Text.UTF8Encoding encoder = new System.Text.UTF8Encoding();
 System.Text.Decoder utf8Decode = encoder.GetDecoder();

        byte[] todecode_byte = Convert.FromBase64String(data);
        int charCount = utf8Decode.GetCharCount(todecode_byte, 0,
todecode_byte.Length);
 char[] decoded_char = new char[charCount];
 utf8Decode.GetChars(todecode_byte, 0, todecode_byte.Length, decoded_char, 0);
        string result = new String(decoded_char);
        return result;
 }
 catch (Exception e)
 {
 throw new Exception("Error in base64Decode" + e.Message);
```

```
}
}
public string base64Encode(string data)
{
// Based on: http://www.vbforums.com/showthread.php?s=&threadid=287324
try
{
byte[] encData_byte = new byte[data.Length];
        encData_byte = System.Text.Encoding.UTF8.GetBytes(data);
        string encodedData = Convert.ToBase64String(encData_byte);
        return encodedData;
}
catch (Exception e)
{
throw new Exception("Error in base64Encode" + e.Message);
}
}
```

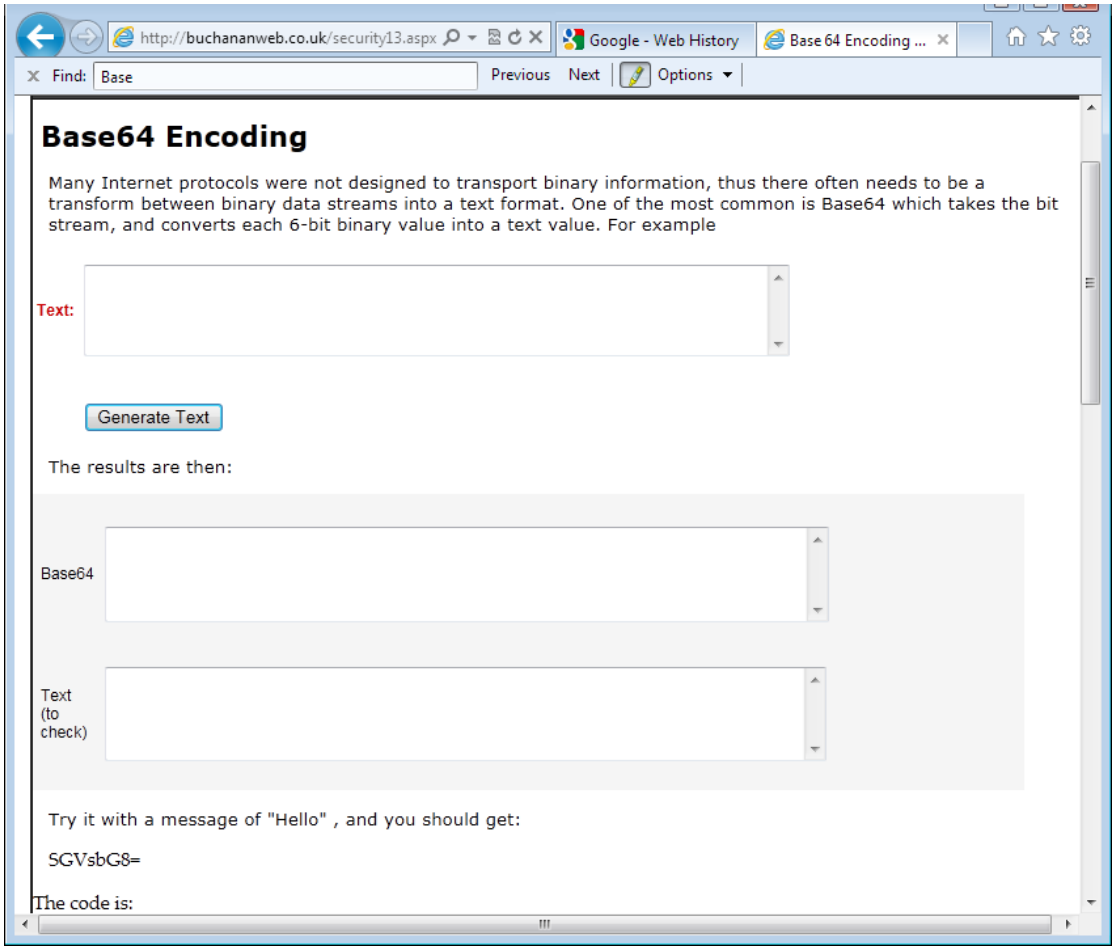

Figure 1:

A.5. Now complete the following table (the first one has been completed for you).

Table 1: Base-64 values

String	Base-64
hello	aGVsbG8=
Napier	
anthill	
forest	
Forest	

A.6. Next implement the page given in (where the code is given at the bottom of the page):

http://buchananweb.co.uk/security14.aspx

A.7. Now complete the following table (the first one has been completed for you). The words should be common words, and should complete a message:

String	Base-64
	UmVtZW1iZXIgdG8=
	ZGVmaW5lIHlvdXIgQVNQWA==
	aW4gYSBmb3JtYXQgd2hpY2ggY2FuIGJl
	aW50ZXJwcmV0ZWQgYnkgSUlTLg==

A.8. Decode this message:

VGhlIFdobyBndWl0YXJpc3QgUGV0ZSBUb3duc2hlbmQgaGFzIHVyZ2VkI
EFwcGxlJ3MgaVR1bmVzIHRvIHVzZSBpdHMgcG93ZXIgdG8gaGVscCBu
ZXcgYmFuZHMgaW5zdGVhZCBvZiAiYmxlZWRpbmciIGFydGlzdHMgbG
lrZSBhICJkaWdpdGFsIHZhbXBpcmUiLgoKVG93bnNoZW5kIG1hZGUgdG
hlIGNvbW1lbnRzIGluIEJCQyA2IE11c2ljJ3MgaW5hdWd1cmFsIEpvaG4gU
GVlbCBMZWN0dXJlLCBuYW1lZCBpbiBob25vdXIgb2YgdGhlIGxlZ2VuZ
GFyeSBESi4KCkhlIGFsc28gYXJndWVkIGFnYWluc3QgdW5hdXRob3Jpc2
VkIGZpbGUtc2hhcmluZywgc2F5aW5nIHRoZSBpbnRlcm5ldCB3YXMgIm
Rlc3Ryb3lpbmcgY29weXJpZ2h0IGFzIHdlIGtub3cgaXQiLgo=

B Private-key encryption

B.1. Implement the following pages, and add the code which performs the encryption and decryption:

3DES http://buchananweb.co.uk/security07.aspx
AES http://buchananweb.co.uk/security15.aspx

The following message was created with the key of "hello" with AES. Can you modify the Web pages so that you can decrypt it:

A1135FD83E128D2BEF34F0AD45D0A0E2364D65B96C535B226BCAB4DE88BA AC2B

C Hashing Methods

C.1. Implement the following page, and add the code which performs the hashing functions:

MD5 http://buchananweb.co.uk/security03.aspx

Next complete Table 2.

Table 2:

String	MD5
Hello	5D41402ABC4B2A76B9719D911017C592
Napier	
Anthill	
Forest	
Forest	

Check these against a tool on the Web, and determine if they match.

D Public-key encryption

D.1. Implement the following page, and add the code which creates a public and private key:

RSA http://buchananweb.co.uk/security18.aspx

Add more prime numbers to the code, and check that it still works.

E Diffie-Hellman

E.1. Implement the following page, and add the code which performs a calculation for Diffie-Hellman, and prove for a number of examples that the same secret key can be created:

RSA http://buchananweb.co.uk/security02.aspx

F Digital Certificates

F.1. Download the following package, and create your own certificate:

http://pcwin.com/Internet/abylon_SELFCERT/download.htm

F.2. Next implement the following page, and add the code which performs which reading your own certificate.

http://buchananweb.co.uk/security10.aspx

Did it manage to read successfully? Yes / No

G Secure Function Evaluation (SFE)

G.1. Implement the following page, and add the code which performs the SFE function, and prove for a number of examples that the total votes are correct:

SFE http://buchananweb.co.uk/security17.aspx

With votes of Bob=5, Alice=6 and Carol=7:

What is the value that Bob calculates?

What is the value that Alice calculates?

What is the value that Carol calculates?

What is the value calculated for the total number of votes?