

For my project this semester I chose to try and implement the Voting System created by Brett Wilson for his Masters Project, "IMPLEMENTING A PAILLIER THRESHOLD CRYPTOGRAPHY SCHEME AS A WEB SERVICE". My initial thought was that I would setup the server and web site and conduct a vulnerability assessment against the service developed by Brett Wilson, but I quickly realized this would end up a vulnerability assessment against IIS, ASP.Net, the .Net framework or poor programming techniques used to create the voting service vs. actually identifying any vulnerabilities with the Paillier Cryptography scheme.

I downloaded the project created by Brett Wilson, this included his paper and the source code used to build the Paillier based Web Services. I created a Windows 2008 Server Virtual Machine running on ESXi 4.1. I turned one of my older computers at home into an ESXi Server, running an Intel Core 2 Duo, Quad Core with 8 Gig of RAM and 1TB HD. The only problem I had was finding a 1GB NIC that would work with this configuration as ESXi does not provide drivers for wireless networks, and understandably so.

After setting up a Windows 2008 Server VM, I had to install IIS, the .Net Framework, Visual Studio, and install and setup Microsoft SQL 2008 Express. Initially I downloaded VS 2010 Express, which caused me numerous problems. Everything installed fine and would have worked great for a development environment using VS 2010, but since the source code created by Brett Wilson was done in VS 2005 I had nothing but problems. Parts of his software are created using VB 2005, Visual C++, and Visual Web Developer using ASP.net 2.0, and didn't port well into VS 2010 Express.

I tried but I could not get the project to import cleanly, and the GNU Multi Precision Library would not import at all. I was having numerous issues trying to load the project into VS. After many days of struggling I discovered that VS 2010 Express doesn't have all the components needed to import the source code and had compatibility issues with the older file extensions. I had multiple other applications that I needed to install in addition to VS 2010 Express as they are not standard in the express package. Some of the additional packages I needed to install included SQL Server Manager, MS Windows SDK for Windows 7, Visual J# Redistributable, and the yasm modular assembler found at the following link - <http://yasm.tortall.net>

In the end I had to rebuild the W2008 Server, reinstall, setup, and/or configure IIS, SQL and VS 2010 Professional that I downloaded from the MS Academic Alliance. Once I installed VS 2010 everything started coming together, I was able to create the database, configure IIS to support the voting sites, create the X.509 Certificates, but could not compile the program due to problems with the GmpGlue.dll that was needed by the application.

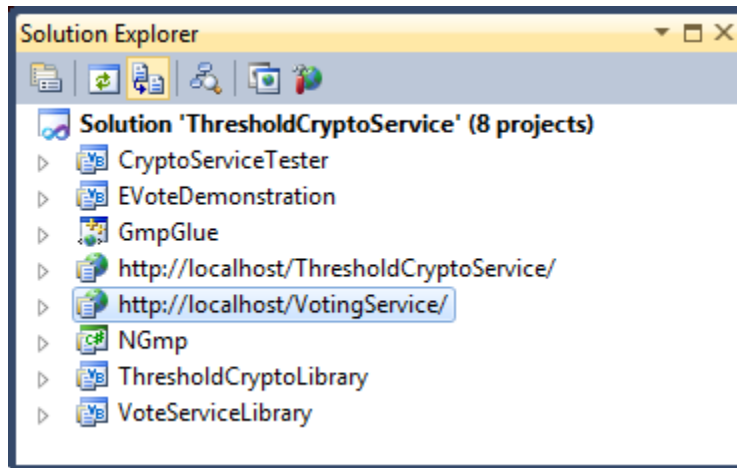
I discovered multiple problems with macros setup within VS C++ for the GmpGlue part of the project. The macros referenced directories on Brett Wilson's computer where he developed the code. I had hosted the source code on my system in a different directory so the compiler

couldn't find all the necessary headers and libraries referenced in the macros. Once I resolved these issues I was able to build the gmpglue.dll and build the project in the debug mode.

The program builds with only a few warnings and will run in debug mode. Below are a few screenshots from the application before it crashes, I've been able to work through some of the crash by fixing bits and pieces of the code, commenting out specific sections just so I could explore and learn more about the application. I had been working my way through numerous crashes but every time I fix one another one shows up. I continued to work my way through the code using the debugger but continue to have problems, first off I'm not very familiar with this application, X.509 Certificates, the libraries and functions called within the program.

I continued to work through these problems and every time I feel I am getting close I end up moving 10 steps back. I have made progress as the program does compile and I can modify the source code. Earlier on I was having issues with not being able to modify 64bit code. I just don't know how long it would take to actually fix every problem. Additionally there simply isn't enough time in a 7 week summer class.

The below snapshot from VS 2010 shows the 6 projects needed by the Threshold Crypto Service and the two web sites that I assume will host the voting service once everything is working on the back end.



Below is a listing of the warnings that I receive when I build the application.

```
----- Build started: Project: NGmp, Configuration: Release Any CPU -----
NGmp -> C:\inetpub\wwwroot\bswilson\src1\project\VS2005\NGmp\NGmp-
0.5.0.10\NGmp\bin\Release\NGmp.dll
----- Build started: Project: ThresholdCryptoLibrary, Configuration: Release Any CPU -----
C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\ThresholdCryptoLibrary\
PaillierThresholdCryptoServiceProvider.vb(389) : warning BC42104: Variable 'cert' is used
before it has been assigned a value. A null reference exception could result at runtime.
C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\ThresholdCryptoLibrary\
PaillierThresholdCryptoServiceProvider.vb(414) : warning BC42107: Property
'CspKeyContainerInfo' doesn't return a value on all code paths. A null reference exception
could occur at run time when the result is used.
C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\ThresholdCryptoLibrary\
PaillierThresholdCryptoServiceProvider.vb(419) : warning BC42105: Function 'ExportCspBlob'
```

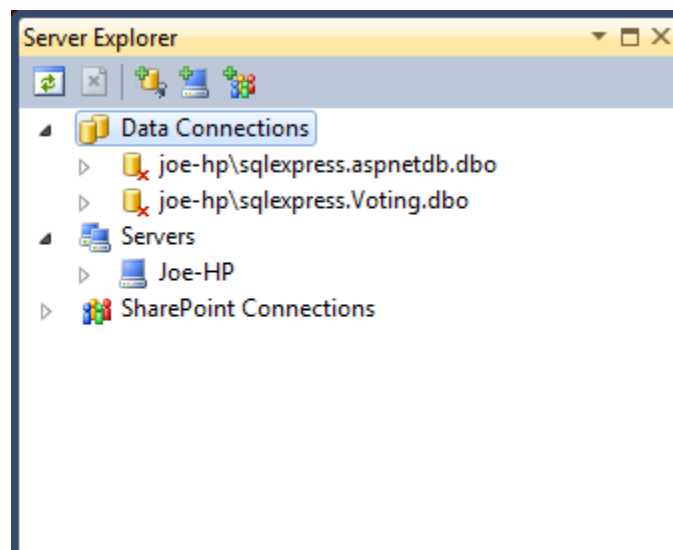
```

doesn't return a value on all code paths. A null reference exception could occur at run time
when the result is used.
C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\ThresholdCryptoLibrary\
Utilities.vb(4) : warning BC40056: Namespace or type specified in the Imports 'java.math'
doesn't contain any public member or cannot be found. Make sure the namespace or the type is
defined and contains at least one public member. Make sure the imported element name doesn't
use any aliases.
ThresholdCryptoLibrary ->
C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\ThresholdCryptoLibrary\
bin\Release\ThresholdCryptoLibrary.dll
----- Build started: Project: VoteServiceLibrary, Configuration: Release Any CPU -----
VoteServiceLibrary ->
C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\VoteServiceLibrary\bin\
Release\VoteServiceLibrary.dll
----- Build started: Project: EVoteDemonstration, Configuration: Release Any CPU -----
C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\EVoteDemonstration\Requ
estBuilder.vb(140) : warning BC42104: Variable 'cert' is used before it has been assigned a
value. A null reference exception could result at runtime.
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Microsoft.Common.targets(2580,9): warning
MSB3187: Referenced assembly 'C:\inetpub\wwwroot\bswilson\src1\project\VS2005\NGmp\NGmp-
0.5.0.10\NGmp\bin\Release\NGmp.dll' targets a different processor than the application.
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Microsoft.Common.targets(2580,9): warning
MSB3187: Referenced assembly
'C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\ThresholdCryptoLibrary
\bin\Release\ThresholdCryptoLibrary.dll' targets a different processor than the application.
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Microsoft.Common.targets(2580,9): warning
MSB3187: Referenced assembly
'C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\VoteServiceLibrary\bin
\Release\VoteServiceLibrary.dll' targets a different processor than the application.
EVoteDemonstration ->
C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\EVoteDemonstration\bin\
Release\EVoteDemonstration.exe
===== Build: 4 succeeded or up-to-date, 0 failed, 0 skipped =====

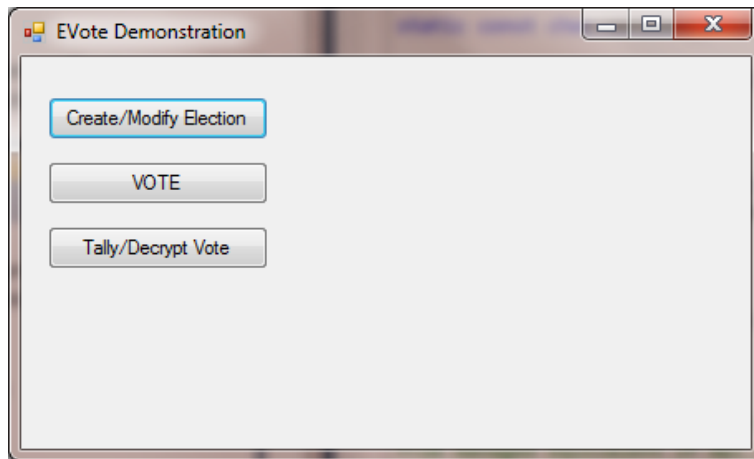
```

The other applications didn't need to build as there were already up to date.

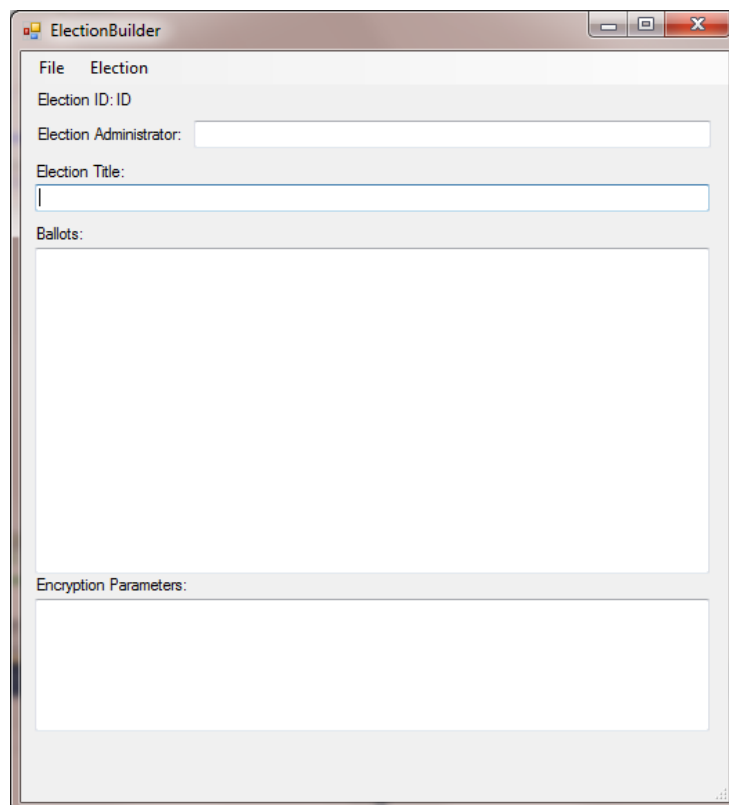
Below is a snapshot of the Server Explorer window that shows the connection to the voting and aspnet databases created within SQL Express.



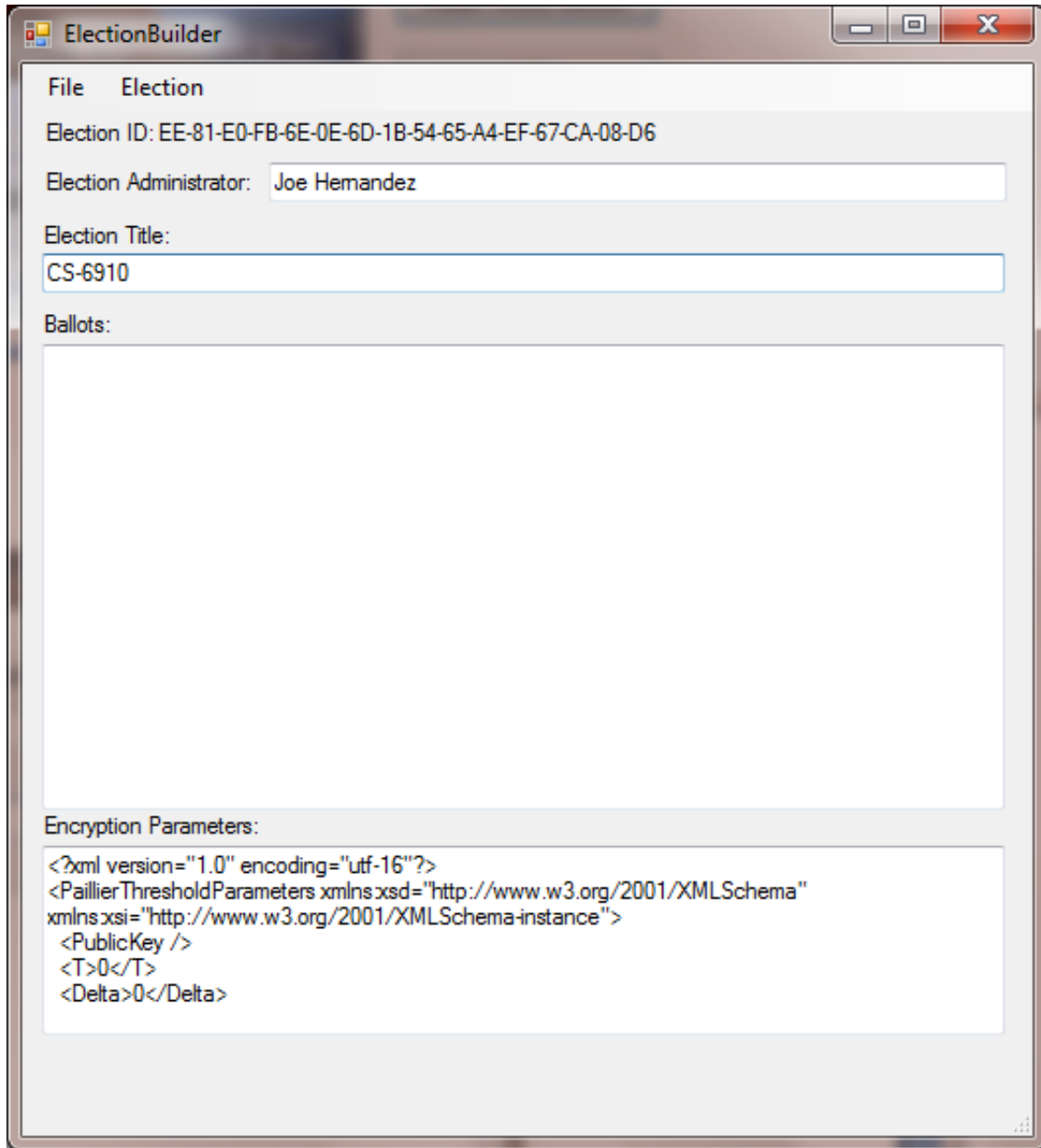
Once the application builds it runs the EVote Demonstration window. This window will allow a user to create or modify an election, cast a vote and tally, decrypt votes.



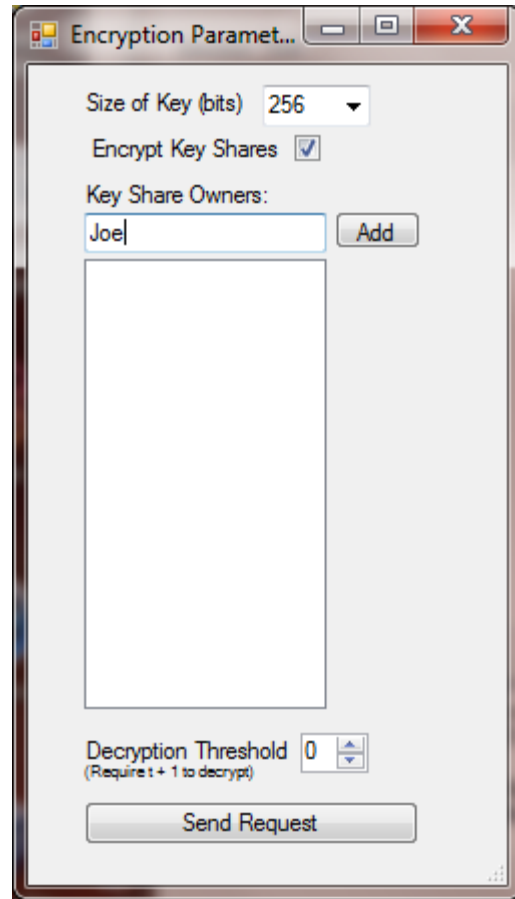
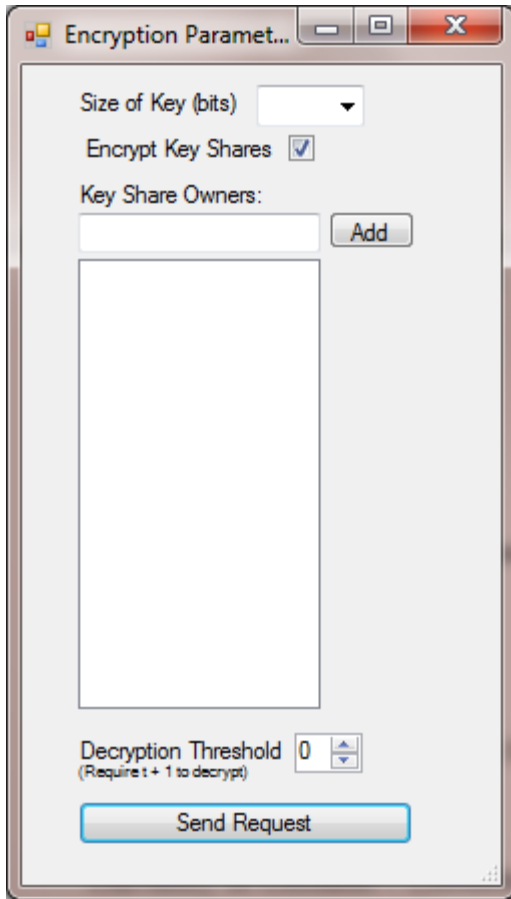
Selecting the Create/Modify Election opens the Election Builder window shown below.



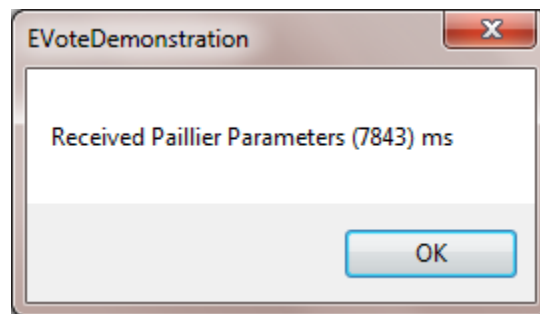
Selecting File -> New Election will populate the Election ID: with an encryption string and also create Encryption Parameters as demonstrated in the window below.



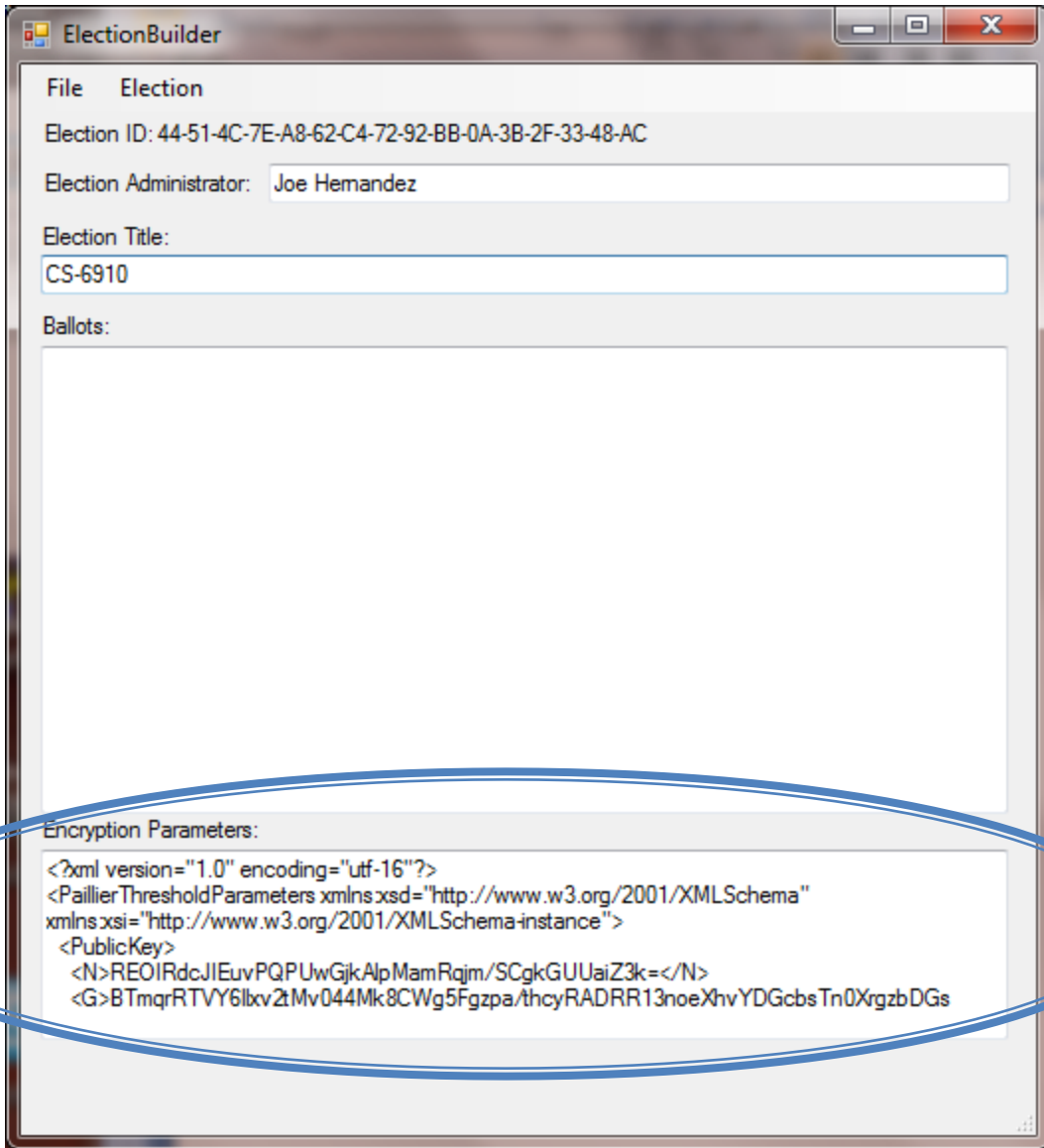
I am able to add an Election Administrator and Election Title then save the election by selecting File -> Save. Once the election has been saved two of the options under the Elections Tab are now accessible. Get Encryption Parameters and Post Election to Voting Service, the other two options, Add Ballot and Create Ballot are still grayed out. Selecting Get Encryption Parameters opens the Encryption Parameters window.



Setting the Size of Key (Bits) Field to anything other than 256 causes the system to crash, but with a setting of 256 and a Decryption Threshold of "0" the application doesn't crash when clicking the Send Request button. The following window pops up, clicking the OK button returns to the Election Builder Window.

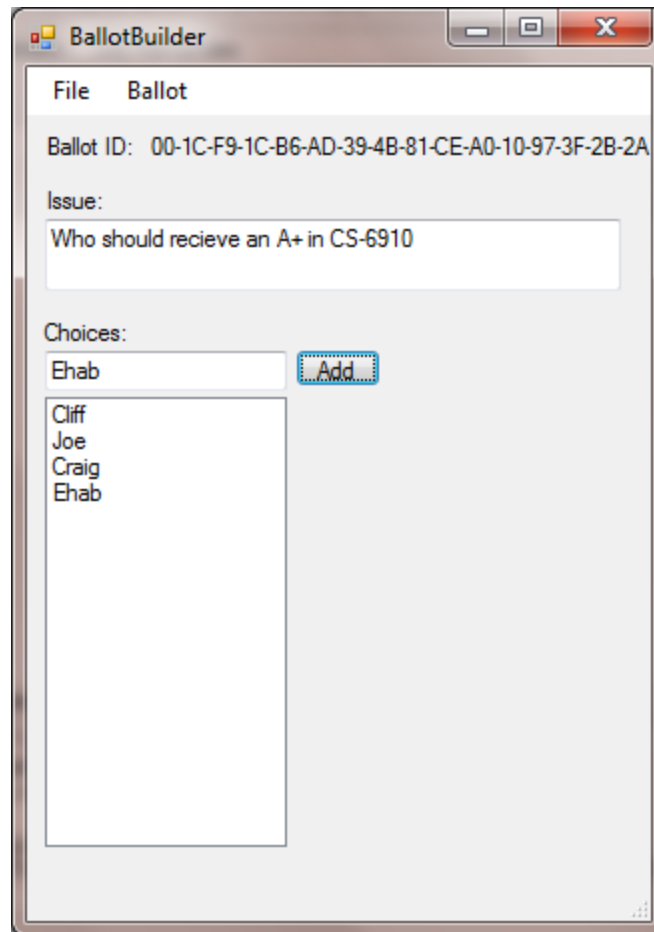


This time in the Election Builder window the Encryption Parameters window now contains a Public Key: N, G and Theta as shown below, Theta is not shown in the window but is there when the XML election file is reviewed. The XML election file is shown later in this document.



At this point the two other options under the Elections Tab, Add Ballot and Create Ballot are now able to be selected.

Selecting Elections-> Create Ballot opens the BallotBuilder window that allows a ballot to be created based on an issue and choices that can be added to the ballot. The File tab allows for the ballot to be saved and then added to the election in the Election Builder window.



Saving the ballot creates the following XML file.

```
<?xml version="1.0" encoding="UTF-8"?>
- <Ballot xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <BallotID>ABz5HLatOUuBzqAQIz8rKg==</BallotID>
  <Issue>Who should recieve an A+ in CS-6910</Issue>
  - <Candidates>
    - <Candidate>
      <Name>Cliff</Name>
      <VoteValueExp>0</VoteValueExp>
    </Candidate>
    - <Candidate>
      <Name>Joe</Name>
      <VoteValueExp>0</VoteValueExp>
    </Candidate>
    - <Candidate>
      <Name>Craig</Name>
      <VoteValueExp>0</VoteValueExp>
    </Candidate>
    - <Candidate>
      <Name>Ehab</Name>
      <VoteValueExp>0</VoteValueExp>
    </Candidate>
  </Candidates>
</Ballot>
```


But when I tried to add the ballot to the election in the Election Builder window the system crashed and I received the following error message within VS debug mode.

System.BadImageFormatException was unhandled

Message=An attempt was made to load a program with an incorrect format. (Exception from HRESULT: 0x8007000B)

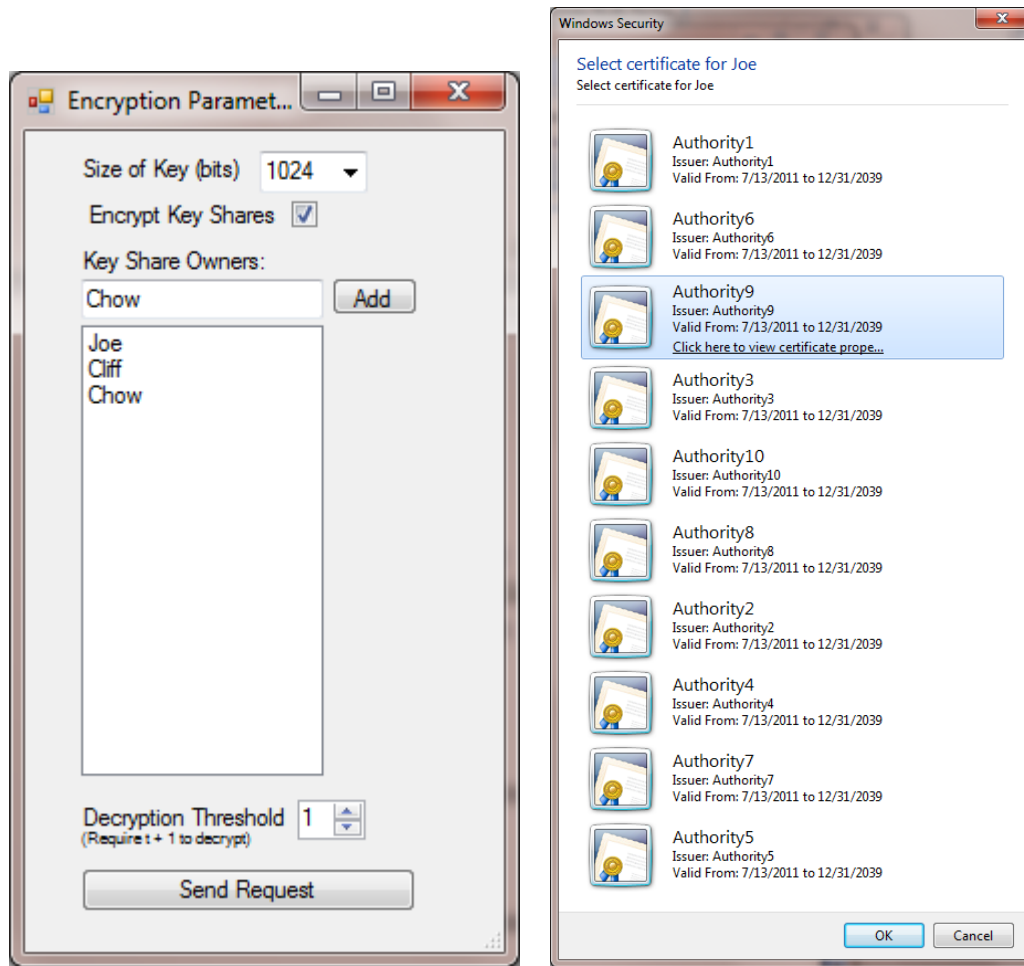
Source=NGmp

StackTrace:

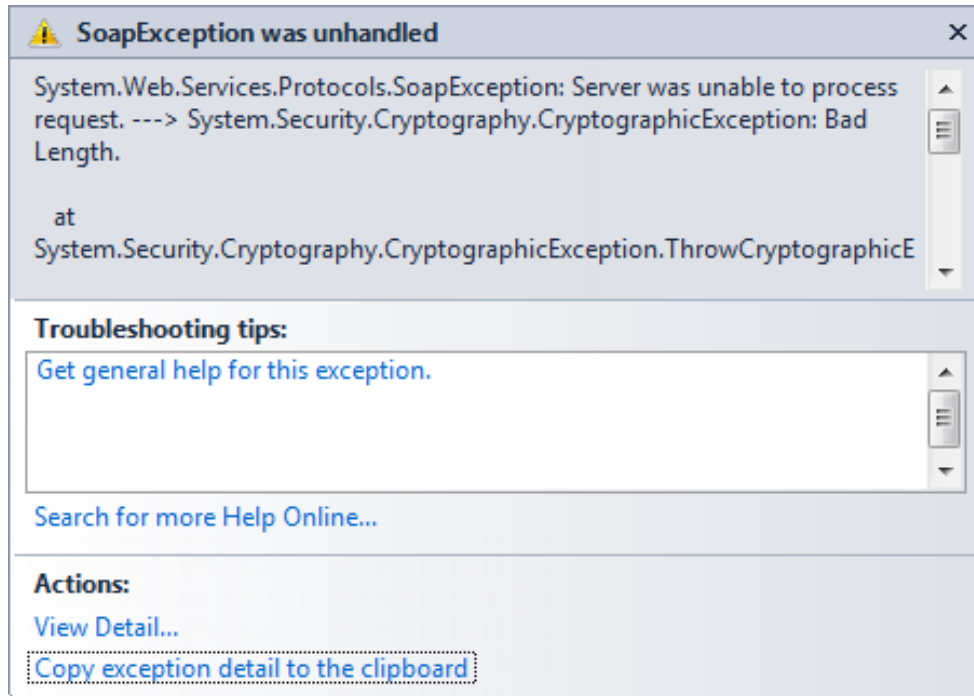
```
    at NGmp.Math.IntMP.__gmpz_init(IntPtr integer)
    at NGmp.Math.IntMP..ctor() in C:\inetpub\wwwroot\bswilson\src1\project\VS2005\NGmp\NGmp-0.5.0.10\NGmp\IntMP.cs:line 72
    at Barleydog.VotingService.ElectionBuilder.AddBallotToolStripMenuItem_Click(Object sender, EventArgs e) in C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\EVoteDemonstration\ElectionBuilder.vb:line 121
    at System.Windows.Forms.ToolStripItem.OnClick(EventArgs e)
    at System.Windows.Forms.ToolStripItem.HandleClick(EventArgs e)
    at System.Windows.Forms.ToolStripItem.HandleMouseUp(MouseEventArgs e)
    at System.Windows.Forms.ToolStripItem.OnMouseUp(MouseEventArgs mea)
    at System.Windows.Forms.ToolStripItemDropDown.OnMouseUp(MouseEventArgs mea)
    at System.Windows.Forms.Control.WmMouseUp(Message& m, MouseButton button, Int32 clicks)
    at System.Windows.Forms.Control.WndProc(Message& m)
    at System.Windows.Forms.ToolStripItem.WndProc(Message& m)
    at System.Windows.Forms.ToolStripItemDropDown.WndProc(Message& m)
    at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr hWnd, Int32 msg, IntPtr wparam, IntPtr lparam)
    at System.Windows.Forms.UnsafeNativeMethods.DispatchMessageW(MSG& msg)
    at
System.Windows.Forms.Application.ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushMessageLoop(IntPtr dwComponentID, Int32 reason, Int32 pvLoopData)
    at System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner(Int32 reason, ApplicationContext context)
    at System.Windows.Forms.Application.ThreadContext.RunMessageLoop(Int32 reason, ApplicationContext context)
    at System.Windows.Forms.Form.ShowDialog(IWin32Window owner)
    at Barleydog.VotingService.EvoteDemonstration.Button1_Click(Object sender, EventArgs e) in C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\EVoteDemonstration\EvoteDemonstration.vb:line 7
    at System.Windows.Forms.Button.OnMouseUp(MouseEventArgs mevent)
    at System.Windows.Forms.Control.WmMouseUp(Message& m, MouseButton button, Int32 clicks)
    at System.Windows.Forms.Control.WndProc(Message& m)
    at System.Windows.Forms.ButtonBase.WndProc(Message& m)
    at System.Windows.Forms.Button.WndProc(Message& m)
```

at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr hWnd, Int32 msg, IntPtr wparam, IntPtr lparam)
at System.Windows.Forms.UnsafeNativeMethods.DispatchMessageW(MSG& msg)
at
System.Windows.Forms.Application.ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushMessageLoop(IntPtr dwComponentID, Int32 reason, Int32 pvLoopData)
at System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner(Int32 reason, ApplicationContext context)
at System.Windows.Forms.Application.ThreadContext.RunMessageLoop(Int32 reason, ApplicationContext context)
at Microsoft.VisualBasic.ApplicationServices.WindowsFormsApplicationBase.OnRun()
at Microsoft.VisualBasic.ApplicationServices.WindowsFormsApplicationBase.DoApplicationModel()
at Microsoft.VisualBasic.ApplicationServices.WindowsFormsApplicationBase.Run(String[] commandLine)
at Barleydog.VotingService.My.MyApplication.Main(String[] Args) in 17d14f5c-a337-4978-8281-53493378c1071.vb:line 81
at System.AppDomain._nExecuteAssembly(RuntimeAssembly assembly, String[] args)
at Microsoft.VisualStudio.HostingProcess.HostProc.RunUsersAssembly()
at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state, Boolean ignoreSyncCtx)
at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state)
at System.Threading.ThreadHelper.ThreadStart()
InnerException:

Playing around with the application some more, setting a Size of Key (bits) to 1024 checking the Encrypt Key Shares, entering a name and selecting Add



An X.509 certificate can be selected for each Key Share Owner as shown in the Windows Security window shown to the right above. This allows a certificate to be assigned to the owner, these certificates were created by running the "CreateTestCertificates.bat" batch file during the programs setup. This batch file must be run from the VS command prompt. Clicking the Send Request button generates the following program crash.



System.Web.Services.Protocols.SoapException was unhandled

Actor=""

Lang=""

Message=System.Web.Services.Protocols.SoapException: Server was unable to process request. --->
System.Security.Cryptography.CryptographicException: Bad Length.

at System.Security.Cryptography.CryptographicException.ThrowCryptographicException(Int32 hr)
at System.Security.Cryptography.RSACryptoServiceProvider.EncryptKey(SafeKeyHandle pKeyContext, Byte[]
pbKey, Int32 cbKey, Boolean fOAEP, ObjectHandleOnStack ohRetEncryptedKey)
at System.Security.Cryptography.RSACryptoServiceProvider.Encrypt(Byte[] rgb, Boolean fOAEP)
at
Barleydog.ThresholdCryptography.ThresholdCryptoService.GeneratePaillierThresholdParameters(ThresholdParam
eterRequest request) in
C:\inetpub\wwwroot\bswilson\src1\project\ThresholdCryptoService\App_Code\ThresholdCryptoService.vb:line
34

--- End of inner exception stack trace ---

Node=""

Role=""

Source=System.Web.Services

StackTrace:

at System.Web.Services.Protocols.SoapHttpClientProtocol.ReadResponse(SoapClientMessage message,
WebResponse response, Stream responseStream, Boolean asyncCall)

at System.Web.Services.Protocols.SoapHttpClientProtocol.Invoke(String methodName, Object[] parameters)

at
Barleydog.VotingService.localhost.ThresholdCryptographyService.GeneratePaillierThresholdParameters(ThresholdParameterRequest request) in
C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\EVoteDemonstration\WebReferences\localhost\Reference.vb:line 80

at Barleydog.VotingService.RequestBuilder.btnSendRequest_Click(Object sender, EventArgs e) in
C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\EVoteDemonstration\RequestBuilder.vb:line 38

at System.Windows.Forms.Button.OnMouseUp(MouseEventArgs mevent)

at System.Windows.Forms.Control.WmMouseUp(Message& m, MouseButtons button, Int32 clicks)

at System.Windows.Forms.Control.WndProc(Message& m)

at System.Windows.Forms.ButtonBase.WndProc(Message& m)

at System.Windows.Forms.Button.WndProc(Message& m)

at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr hWnd, Int32 msg, IntPtr wparam, IntPtr lparam)

at System.Windows.Forms.UnsafeNativeMethods.DispatchMessageW(MSG& msg)

at
System.Windows.Forms.Application.ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushMessageLoop(IntPtr dwComponentID, Int32 reason, Int32 pvLoopData)

at System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner(Int32 reason, ApplicationContext context)

at System.Windows.Forms.Application.ThreadContext.RunMessageLoop(Int32 reason, ApplicationContext context)

at System.Windows.Forms.Form.ShowDialog(IWin32Window owner)

at Barleydog.VotingService.ElectionBuilder.GetEncryptionParametersToolStripMenuItem_Click(Object sender, EventArgs e) in
C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\EVoteDemonstration\ElectionBuilder.vb:line 165

at System.Windows.Forms.ToolStripItem.OnClick(EventArgs e)

at System.Windows.Forms.ToolStripItem.HandleClick(EventArgs e)

at System.Windows.Forms.ToolStripItem.HandleMouseUp(MouseEventArgs e)

at System.Windows.Forms.ToolStripItem.OnMouseUp(MouseEventArgs mea)

at System.Windows.Forms.ToolStripItemDropDown.OnMouseUp(MouseEventArgs mea)

at System.Windows.Forms.Control.WmMouseUp(Message& m, MouseButtons button, Int32 clicks)

at System.Windows.Forms.Control.WndProc(Message& m)

at System.Windows.Forms.ToolStripItem.WndProc(Message& m)

at System.Windows.Forms.ToolStripItemDropDown.WndProc(Message& m)

at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr hWnd, Int32 msg, IntPtr wparam, IntPtr lparam)

at System.Windows.Forms.UnsafeNativeMethods.DispatchMessageW(MSG& msg)

at
System.Windows.Forms.Application.ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushMessageLoop(IntPtr dwComponentID, Int32 reason, Int32 pvLoopData)

at System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner(Int32 reason, ApplicationContext context)

at System.Windows.Forms.Application.ThreadContext.RunMessageLoop(Int32 reason, ApplicationContext context)

at System.Windows.Forms.Form.ShowDialog(IWin32Window owner)

at Barleydog.VotingService.EvoteDemonstration.Button1_Click(Object sender, EventArgs e) in C:\inetpub\wwwroot\bswilson\src1\project\VS2005\ThresholdCryptoService\EVoteDemonstration\EvoteDemonstration.vb:line 7

at System.Windows.Forms.Button.OnMouseUp(MouseEventArgs mevent)

at System.Windows.Forms.Control.WmMouseUp(Message& m, MouseButtons button, Int32 clicks)

at System.Windows.Forms.Control.WndProc(Message& m)

at System.Windows.Forms.ButtonBase.WndProc(Message& m)

at System.Windows.Forms.Button.WndProc(Message& m)

at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr hWnd, Int32 msg, IntPtr wparam, IntPtr lparam)

at System.Windows.Forms.UnsafeNativeMethods.DispatchMessageW(MSG& msg)

at System.Windows.Forms.Application.ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushMessageLoop(IntPtr dwComponentID, Int32 reason, Int32 pvLoopData)

at System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner(Int32 reason, ApplicationContext context)

at System.Windows.Forms.Application.ThreadContext.RunMessageLoop(Int32 reason, ApplicationContext context)

at Microsoft.VisualBasic.ApplicationServices.WindowsFormsApplicationBase.OnRun()

at Microsoft.VisualBasic.ApplicationServices.WindowsFormsApplicationBase.DoApplicationModel()

at Microsoft.VisualBasic.ApplicationServices.WindowsFormsApplicationBase.Run(String[] commandLine)

at Barleydog.VotingService.My.MyApplication.Main(String[] Args) in 17d14f5c-a337-4978-8281-53493378c1071.vb:line 81

at System.AppDomain._nExecuteAssembly(RuntimeAssembly assembly, String[] args)

at Microsoft.VisualStudio.HostingProcess.HostProc.RunUsersAssembly()

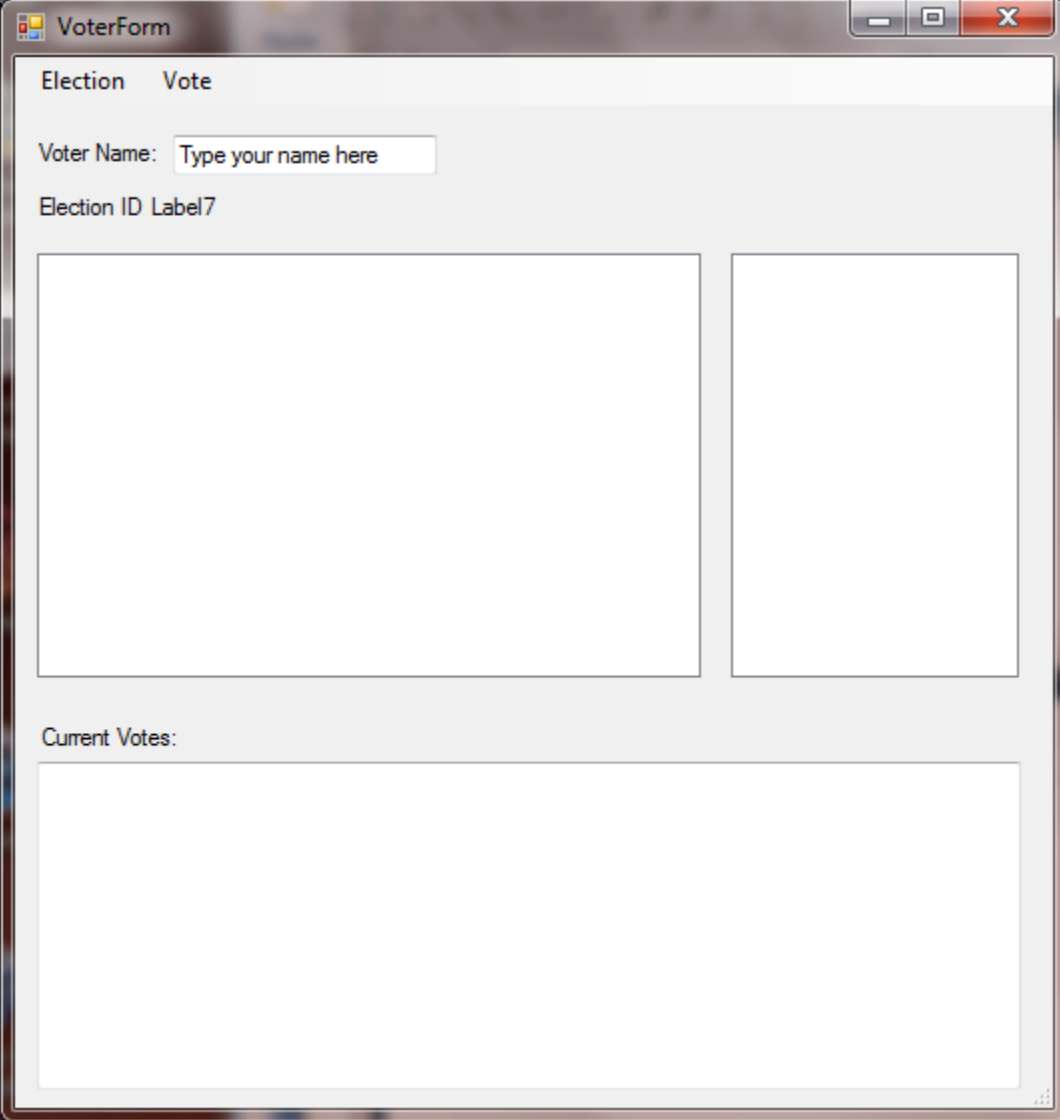
at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state, Boolean ignoreSyncCtx)

at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state)

at System.Threading.ThreadHelper.ThreadStart()

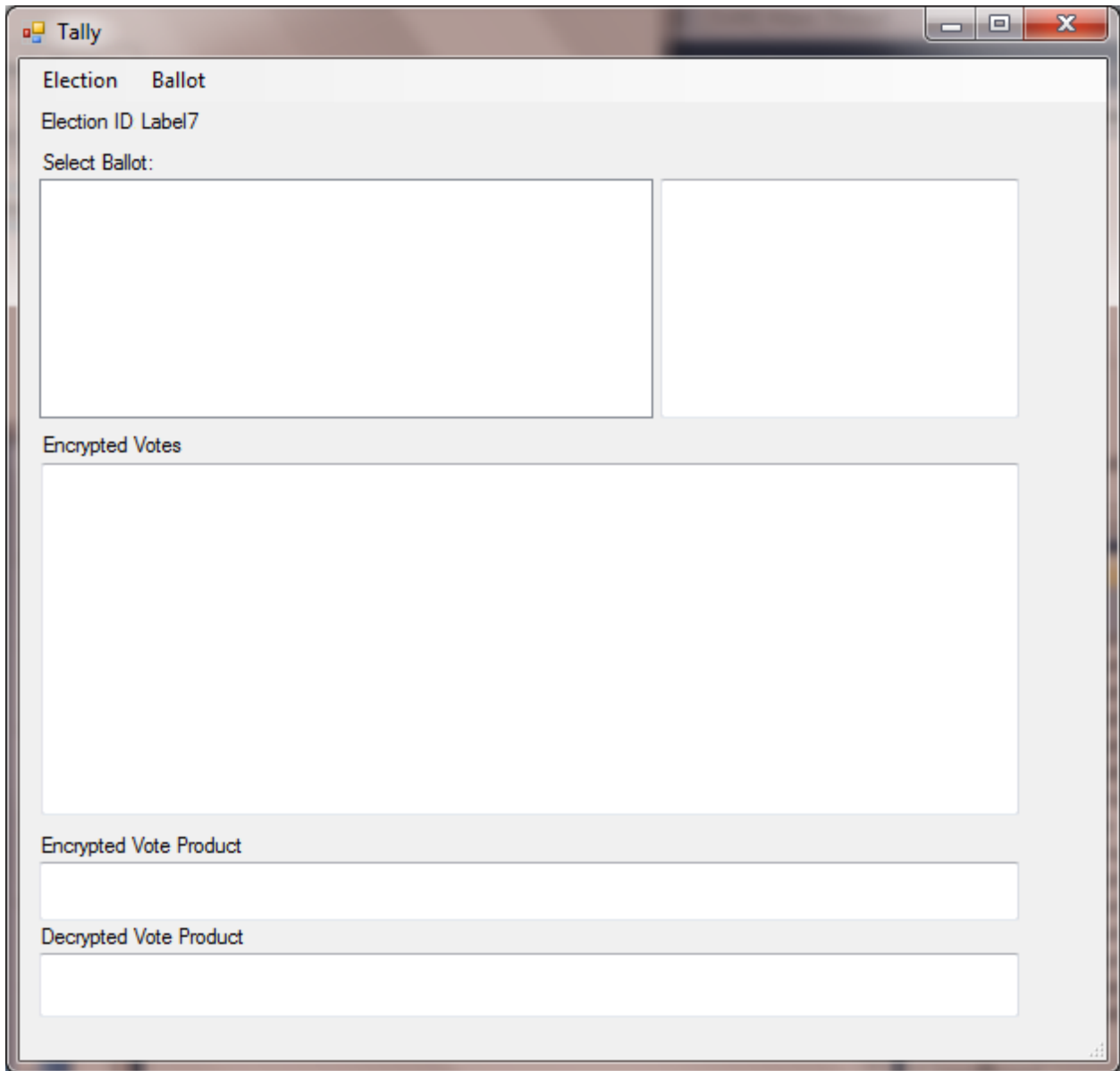
InnerException:

At this point I have run out of time and needed to start building my report. In this class there wasn't enough time for me to continue working on this project, with no end in site. But I was able to open these other forms, VoterForm and Tally Election, shown below.



The image shows a screenshot of a Windows application window titled "VoterForm". The window has a standard Windows title bar with minimize, maximize, and close buttons. The main content area of the window is light gray and contains the following elements:

- At the top left, the text "Election" and "Vote" are displayed.
- Below that, the text "Voter Name:" is followed by a text input field containing the placeholder text "Type your name here".
- Below the input field, the text "Election ID Label7" is displayed.
- Underneath "Election ID Label7", there are two empty rectangular boxes side-by-side, likely intended for displaying data or images.
- At the bottom of the window, the text "Current Votes:" is displayed above a large, empty rectangular area, likely intended for displaying a list of votes or a summary.



The following XML is the data file from one of the elections I was able to save before the system crashed. On subsequent runs I was able to load the election, but when I proceeded I still encountered the same program crashes.


```

<?xml version="1.0" encoding="UTF-8"?>
- <Election xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <ElectionID>RFFMfqhixHKSuwo7LzNIrA==</ElectionID>
  <Title>CS-6910</Title>
  <Administrator>Joe Hernandez</Administrator>
  <Ballots/>
  - <EncryptionParameters>
    - <PublicKey>
      <N>REOIRdcJIEuvPQPUwGjkAlpMamRqjm/SCgkGUUaiZ3k=</N>
      <G>BTmqrRTVY6Ilxv2tMv044Mk8CWg5Fgzpa/thcyRADRR13noeXhvYDGcbsTn0XrgzbDGs+2aRUeFB/0PRIu51sA==</G>
      <Theta>HhGBbxJx63xP9p6DK0u4zt4VOKtt+kVEX9iBvlcP7SU=</Theta>
    </PublicKey>
    - <VerificationKeys>
      - <PaillierThresholdVerificationKey>
        <VerificationKeyBase>/luGauXOmA9Tdf6pzVz28Qih2n2jbc8oKujRMf3JJl8H1FRjNunfTMsMbDj0sLrSGORNR2YOn19m566xYXk</VerificationKeyBase>
        <VerificationKey>CgO4X+Cyo8MHTcrvfXiwuZiK0+uPGQZ8IS9MeHk35yFhXuGUOmint57hcgwuHnOHAYLcsFoxifnzPyIirIzcTQ==</VerificationKey>
      </PaillierThresholdVerificationKey>
    </VerificationKeys>
    - <ThresholdKeyShares>
      - <PaillierThresholdKeyShare>
        - <OwnerInfo>
          <OwnerName>Joe</OwnerName>
          <OwnerX509>MIIB8TCCAV6gAwIBAgIQm6tZHOiosaRDBX3JdYbWuzAJBgUrDgMCHQUAMBUxEzARBgNVBAMTCkF1dGhvcml0eTEwHhcNMTEwNzEzODExWhcNMzk
          </OwnerInfo>
        - <SecretKeyShare>
          <ShareIndex>1</ShareIndex>
          <SecretShare>MCFIiSB4FYwrXT52I+QX41VWYwN/PZOpcBwntG+RCogc/X43rXk7Vs9cxAWsHbVNeqi73ouYINDSWQkGu26VWv/IAGaeZ/xmTYjrjtFKR5l1atWEHnmpjn
          <Encrypted>true</Encrypted>
        </SecretKeyShare>
      </PaillierThresholdKeyShare>
    </ThresholdKeyShares>
    <T>0</T>
    <Delta>1</Delta>
  </EncryptionParameters>
</Election>

```

In conclusion, I believe there are significant differences in specific variables, libraries, functions, the .net Framework, and ASP.net that it would take an experienced programmer to either debug the code or update the specific sections in order to make the program work. Additionally the code is not commented very well so it makes it a bit difficult to understand how everything works. I've actually been having a lot of fun and learning a lot with this project. I think I will continue to work on this in my spare time, eventually I'll understand enough that I may be able to make the updates myself.