(a) Based on the SOAP envelope as shown in p.32 and p.33 of your notes, answer the following questions:

(i) Give the first 4 characters of the encrypted symmetric key.

(ii) Give the XML statement that indicates the algorithm used to encrypt the symmetric key.

(iii) Give the XML statement that indicates the identifier of the public key used to encrypt the symmetric key.

(iv) Give the first 4 characters of the encrypted credit card info.

(v) How does the recipient of this message know the credit card info is encrypted using the symmetric key as defined in `<EncryptedKey>`?
(b) Based on the SOAP envelope as shown in p.35 to p.42 of your notes, answer the following questions:

(i) Which security technologies have been adopted in that SOAP envelope?

(ii) How does the recipient of this message know which public key should be used to decrypt the encrypted digest?

(iii) Give the first 4 characters of the digest.

(iv) Give the statement that indicates the algorithm used to encrypt the `<SignedInfo>` subtree.

(v) Give the algorithm used to canonicalize the `<SignedInfo>` subtree before encrypting it.

(10 marks)
(a) Based on the SOAP envelope as shown in p.32 and p.33 of your notes, answer the following questions:

(i) Give the first 4 characters of the encrypted symmetric key.
   cdck

(ii) Give the XML statement that indicates the algorithm used to encrypt the symmetric key.

   <EncryptionMethod Algorithm =
   "http://www.w3.org/2001/04/xmlenc#rsa-1_5">
   
   </EncryptionMethod>

(iii) Give the XML statement that indicates the identifier of the public key used to encrypt the symmetric key.

   <wsse:KeyIdentifier>u3AA1M+DMOA1bX/vWJ ... 

   </wsse:KeyIdentifier>

(iv) Give the first 4 characters of the encrypted credit card info.

   Ew7Z

(v) How does the recipient of this message know the credit card info is encrypted using the symmetric key as defined in <EncryptedKey>?

   <EncryptedData> has an ID attributed with value “myToken”, which is the same as the one in the <ReferenceList>.

(10 marks)
Based on the SOAP envelope as shown in p.35 to p.42 of your notes, answer the following questions:

(i) Which security technologies have been adopted in that SOAP envelope?

**BinarySecurityToken and XML Digital Signature**

(ii) How does the recipient of this message know which public key should be used to decrypt the encrypted digest?

_It is indicated in the X.509 certificate and sent to the server._

(iii) Give the first 4 characters of the digest.

_Ojjw_

(iv) Give the statement that indicates the algorithm used to encrypt the `<SignedInfo>` subtree.

```xml
<SignatureMethod Algorithm =
  "http://www.w3.org/2000/09/xmlsig#rsa-sha1"/>
```

(v) Give the algorithm used to canonicalize the `<SignedInfo>` subtree before encrypting it.

_excl4n_

(10 marks)