Signature Utility Library

Signature Utility Library for Xml Digital Signature and Cipher functions. By using this library user can sign and verify xml file and encrypt and decrypt the text.

Xml Signature Algorithms:

Signature Method Algorithm	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Digest Method Algorithm	http://www.w3.org/2001/04/xmlenc#sha256

Key Details:

Algorithm	RSA
Key size	2048
Signature algorithm	sha256RSA
Signature Hash Algorithm	Sha256

Classes:

- XmlDigitalSigner
- VerifyDigitalSign
- CipherUtil

XmlDigitalSigner:

By Using this class user can Sign Xml, this class has constructor while creating class object user has to pass the PrivateKey. By passing Xml Document user can invoke generateDigitalSignature(document) and it will return the signed xml.

Sample Code:

```
XmlDigitalSigner signer = new XmlDigitalSigner(privateKey);

String signed=signer.generateDigitalSignature(doc) ;
```

VerifyDigitalSign:

By using this class user can verify the signed xml , this class has constructor which takes PublicKey as parameter.By passing Xml Document user can invoke isXmlDigitalSignatureValid(document) and it will return the boolean value .If validation is success boolean value is true else boolean value is false.

Sample code:

```
VerifyDigitalSign ver = new VerifyDigitalSign(publicKey);

ver.isXmlDigitalSignatureValid(doc);
```

CipherUtil:

By using this class user can Encrypt and Decrypt text, this class has constructor which takes the Cipher Algorithm as parameter. By passing public key and plaint text user can invoke encrypt(value,publickey) and it will return the encrypted value. By passing private key and encrypted text user can invoke decrypt(value,privatekey) and it will return the plain text. Encrypted value will be in Base64 format.

Sample code:

```
CipherUtil enc = new CipherUtil("RSA");

String encValue = enc.encrypt("lorem ipsum", pubKey);

String decryptValue=enc.decrypt(encValue, privateKey);
```

For more information on Xml Digital Signature refer below links:

- https://docs.oracle.com/javase/8/docs/technotes/guides/security/xmldsig/XMLDigitalSignature.html
- http://www.oracle.com/technetwork/articles/javase/dig-signature-api-140772.html

Note : Make sure while making Document setNameSpaceAware is true.