



PENERAPAN ALGORITMA KRIPTOGRAFI



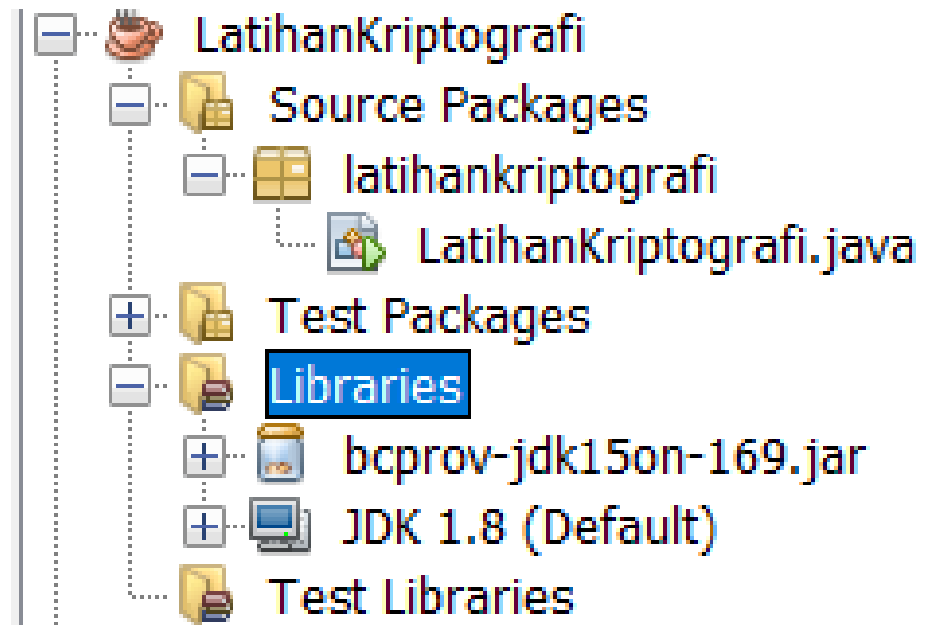
I Komang Setia Buana

Pendahuluan

- Bouncy Castle Crypto API Java menyediakan kriptografi API yang ringan (simple) yang dapat berfungsi mulai dari platform JME hingga JDK 1.7 yang juga sebuah provider untuk Java Cryptography Extension (JCE) dan Java Cryptography Architecture (JCA).
- API Bouncy Castle dapat di download di <https://cloud.poltekssn.ac.id/s/39NpXkcRZo6oSZa>

Praktikum

- Buat project baru dengan nama bebas
- Tambahkan library yang sudah didownload



- Modifikasi kode java dengan menyisipkan kode berikut didalam main
- Jalankan aplikasi

```
Security.addProvider(new org.bouncycastle.jce.provider.BouncyCastleProvider());
byte[] input = "komang".getBytes();
byte[] keyBytes = new byte[] { 0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09,
    0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f };

SecretKeySpec key = new SecretKeySpec(keyBytes, "AES");

Cipher cipher = Cipher.getInstance("AES/ECB/PKCS7Padding", "BC");

System.out.println(new String(input));

// encryption pass
cipher.init(Cipher.ENCRYPT_MODE, key);

byte[] cipherText = new byte[cipher.getOutputSize(input.length)];
int ctLength = cipher.update(input, 0, input.length, cipherText, 0);
ctLength += cipher.doFinal(cipherText, ctLength);
System.out.println(new String(cipherText));
System.out.println(ctLength);

// decryption pass
cipher.init(Cipher.DECRYPT_MODE, key);
byte[] plainText = new byte[cipher.getOutputSize(ctLength)];
int ptLength = cipher.update(cipherText, 0, ctLength, plainText, 0);
ptLength += cipher.doFinal(plainText, ptLength);
System.out.println(new String(plainText));
System.out.println(ptLength);
```

Study kasus membuat aplikasi layanan kriptografi

- Modifikasi tugas program stok barang yang sudah menerapkan client server dengan menambahkan login
- Tambahkan table user didalam database dari program yang sudah dibuat
- Tambahkan form input user didalam aplikasi yang dibuat
- user password yang tersimpan sudah di enkrip sesuai dengan materi diatas
- Tambahkan form login

Tugas

- Deskripsikan hasil praktikum yang dilakukan ke dalam laporan!