Zabavnikova T.Yu. Elements of ergonomics for the problem of interface design. The requirements to convenience and comfort of interface are increasing now, as complexity of works and user's responsibility for the end results increases. In the theses, basic aspects of ergonomic user interface are stated.

Key words: user interface, ergonomics, interface design.

LITERATURE

1. *Romanycheva E.T., Yatsyuk O.G.* Design and advertising // Computer technologies: reference and practical guide. M.: DMK, 2002. 432 pp.
2. *Grozhan D.* Reference book of a designer-beginner (2nd ed.). Rostov-on-Don: Feniks, 2004. 320 pp.
3. *Kirsanov D.* Web-design: Dmitry Kirsanov's Book. SPb: Symbol-Plus, 2007. 368 pp.
4. *Andreev A.* Elaboration of user interface. http//: www.usability.ru

УДК 519.95

ОБ ОДНОМ КРИПТОГРАФИЧЕСКОМ РАСШИРЕНИИ Java

© М.С. Зуев, К.Г. Мирошников

Ключевые слова: криптографические алгоритмы, технология Java.

В статье рассматриваются особенности JCE-библиотеки Bouncycastle. Приводится краткое описание пакетов, входящих в библиотеку Bouncycastle, и пример программы, использующей алгоритм AES для шифрования байтового массива.

В данной статье приводится обзор возможностей одного из пакетов криптографических алгоритмов, предназначенных для java-разработчиков. Наиболее известным таким пакетом является Sun JCE, предоставляющий удобный API для выполнения различных криптографических преобразований. Однако в связи с законами, регулирующими экспорт технологий из США, пакет Sun JCE нельзя загружать и использовать людям, не проживающим на территории США или Канады. Поэтому этот пакет не входит в стандартную поставку Java.

В связи с этим сторонними разработчиками были разработаны аналогичные криптографические пакеты, среди которых часть коммерческих (такие как IAIK JCE, Digt Trusted Java и др.), а другая часть – бесплатные. Одним из самых известных бесплатных решений являлся пакет Cryptix JCE, но его поддержка прекращена с 2005 года. Другим решением является пакет Bouncy Castle, совместимый с новейшими поставками JDK и обладающий следующими основными характеристиками:

– содержит криптографические API для языков Java и C#;
– содержит провайдер для JCE и JCA;
– содержит реализации JCE 1.2.1, реализованные разработчиками самостоятельно (т.е. пакет не содержит кодов JCE 1.2.1 от Sun, следовательно, на него лицензии Sun не распространяются);
– поддерживает спецификации ASN.1 кодирования объектов;
– поддержка сертификатов X.509 различных версий;
– поддержка стандартов Open PGP, OCSP, TSP и др.

Лицензионное соглашение для данного пакета разрешает практически любые действия, включающие передачу, продажу, модификацию, публикацию и др., следовательно, разработчик ПО может свободно использовать все его возможности. Реализации большого количества алгоритмов и протоколов, включая криптоалгоритмы, описанные в документах ГОСТ, делают этот пакет интересным как для разработчиков криптографического ПО, так и для преподавателей по дисциплинам «Криптографическая защита информации» и «Программирование на Java» на специальности «Организация и технология защиты информации».

Библиотека Bouncycastle включает в себя пакеты:

org.bouncycastle.jce – пакет утилит, использующихся с JCE;

org.bouncycastle.openssl – пакет, включающий классы для работы с PEM OpenSSL-файлами;

org.bouncycastle.asn1 – пакет, использующийся для работы с протоколом ASN.1;

org.bouncycastle.crypto – пакет, содержащий основные криптографические алгоритмы;

org.bouncycastle.x509 – пакет, используемый для поддержки X.509 – сертификатов.

Пакет org.bouncycastle.crypto – основной пакет, содержащий реализации различных криптографических алгоритмов. Он содержит следующие подпакеты:

org.bouncycastle.crypto.agreement – пакет, содержащий реализацию протокола Диффи-Хеллмана, включает версию алгоритма с эллиптическими кривыми.

org.bouncycastle.crypto.digests – пакет, содержащий основные классы для вычисления бесключевых хэш-функций сообщений. Включает алгоритмы ГОСТ 34.11-94, MD2, MD4, MD5, Tiger, RIPEMD, SHA разных длин свертки и др.

org.bouncycastle.crypto.encodings – пакет, включающий алгоритмы кодирования информации, предназначенной для обработки асимметричными алгоритмами (например, алгоритм PKCS 1).

org.bouncycastle.crypto.engines – пакет, включающий классы, выполняющие симметричное шифрование. Классы этого пакета позволяют выполнить шифрование массива байтов по алгоритмам ГОСТ 28147-

89, DES, TripleDES, AES, Blowfish, IDEA, RC2, RC4, RC5, RC6, Twofish, Skipjack и мн. др.

org.bouncycastle.crypto.generators – пакет, включающий генераторы ключей, ключевых пар и других параметров криптографических алгоритмов.

org.bouncycastle.crypto.macs – пакет, включающий алгоритмы вычисления ключевых хэш-функций сообщений. Содержит алгоритмы ГОСТ 28147-89 в режиме выработки имитовставки, CMAC, HMAC, а также алгоритм вычисления MAC с использованием любого блочного шифра, обрабатывающего текст блоками методом CBC или CFB.

org.bouncycastle.crypto.modes – пакет, содержащий классы, представляющие способы обработки текста симметричным шифром (например, CBC, CFB, OFB и др.).

org.bouncycastle.crypto.paddings – пакет, предоставляющий различные способы дополнения блоков для симметричных блочных шифров.

org.bouncycastle.crypto.params – пакет, классы которого используются для хранения параметров шифров и генераторов.

org.bouncycastle.crypto.signers – пакет, предоставляющий алгоритмы ЭЦП сообщений. Включает алгоритмы ГОСТ 34.10-91, ГОСТ 34.10-2001, RSA, DSA, EC-DSA и др.

org.bouncycastle.crypto.tls – пакет, обеспечивающий API для TLS.

Приведем пример программы, в которой используются средства пакета Bouncycastle для шифрования байтового массива с помощью алгоритма AES. Программа выполняет шифрование массива байтов toEncrypt с помощью алгоритма AES.

```
BufferedBlockCipher cipher =
new PaddedBufferedBlockCipher( new CBCBlockCipher(new AESFastEngine()));
```

В этой строке создается объект cipher типа BufferedBlockCipher, который представляет шифровальную машину. Алгоритм шифрования – AES, алгоритм обработки блоков – сцепление блоков (CBC).

```
SecureRandom srr = new SecureRandom();
byte [] AESkey = new byte[16];
srr.nextBytes(AESkey);
byte [] AESinitV = new byte[16];
srr.nextBytes(AESinitV);
```

В данном блоке кода инициализируются параметры шифра – ключ и вектор инициализации (IV), требуемый при сцеплении блоков.

```
ParametersWithIV piv= new ParametersWithIV ((new KeyParameter(AESkey)),
AESinitV);
```

В данном блоке кода создается объект типа ParametersWithIV, представляющий параметры шифра, использующего вектор инициализации. Этот объект требуется при инициализации шифра.

```
cipher.init(true, piv);
```

В этой строке инициализируется шифровальная машина. В качестве первого параметра функции init() передается значение true, если шифровальная машина должна работать в режиме шифрования, и false, если шифровальная машина должна работать в режиме расшифрования.

```
byte[] result = new byte[cipher.getOutputSize(
toEncrypt.length)];
```

В этой строке инициализируется массив, в который будет записан шифротекст. Для определения требуемой длины массива выходных данных используется метод getOutputSize().

```
int len = cipher.processBytes(
toEncrypt, 0, toEncrypt.length, result, 0);
```

Метод processBytes() выполняет шифрование массива байт toEncrypt и сохранение результата в массиве result.

```
try {
cipher.doFinal(result, len);
} catch (CryptoException ce) {
result = "Cipher error".getBytes();
ce.printStackTrace();
}
```

Метод doFinal() обрабатывает последний блок буфера шифровальной машины. При возникновении исключений типа CryptoException происходит его перехват и вывод сообщения на экран.

ЛИТЕРАТУРА

1. Java SE security [Электронный ресурс]. Режим доступа: java.sun.com/javase/technologies/security/
2. Bouncycastle Specifications. [Электронный ресурс] Режим доступа: http://www.bouncycastle.org/specifications.html
3. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С. М.: Триумф, 2002. 816 с.

Поступила в редакцию 17 ноября 2008 г.

Zuev M.S., Miroshnikov K.G. On one cryptographic Java expansion. The article considers features of JCE-library Bouncycastle. Short description of packages included into Bouncycastle library and the example of the program, using AES algorithm for byte file enciphering is given.

Key words: cryptographic algorithms, Java technology.

LITERATURE

1. Java SE security [Electronic resource]. Access mode:
2. java.sun.com/javase/technologies/security/
3. Bouncycastle Specifications. [Electronic resource] Access mode: http://www.bouncycastle.org/specifications.html
4. *Shnayer B.* Applied cryptography. Protocols, algorithms, original texts in language C. M.: Triumph, 2002. 816 pp.