# MTAT.07.017
# Applied Cryptography

Rakenduslik krüptograafia
Прикладная криптография

Juri Hudolejev
University of Tartu
Spring 2011

# Topics for This Week

ASN.1 Primitive and Constructed Types

ASN.1 Examples

**`org.bouncycastle.asn1.*`**

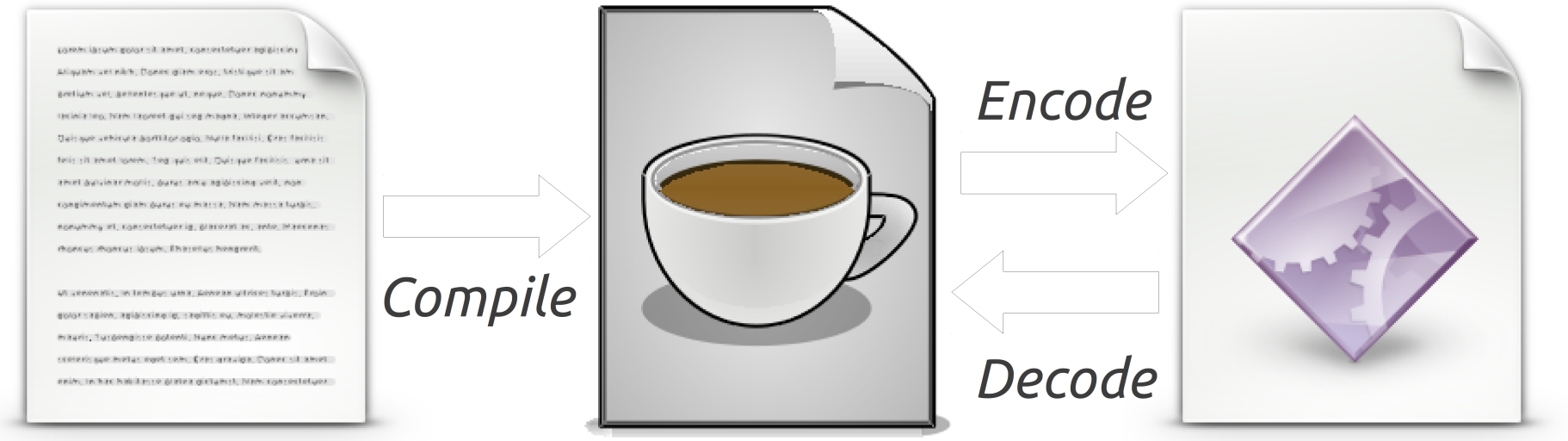
# ASN.1 Usage

```
-- ASN.1 specification
foo SEQUENCE ::= { … }

// Language-specific implementation
foo = ASN1Sequence.getInstance(obj);

# Byte-level representation
10 0c 0c 09 47 6f 6f 64 20 6c 75 63 6b
```

# ASN.1 Usage

ASN.1 spec

Encoded data




Java program

# ASN.1 Simple Types

```
NULL -- only possible value is Null

BOOLEAN -- True or False

INTEGER -- whole numbers -∞..+∞

REAL -- (mantissa, base, exponent)
```

# ASN.1 Usage Examples

```
-- Type description
Gender ::= INTEGER {
    female (1),
    male (2)
}

-- Value assignment
version INTEGER ::= 4
```

# ASN.1 Simple Types

```
BIT STRING -- 0-s and 1-s
OCTET STRING -- values 0x00..0xff

NumericString -- [space]0123456789

UTF8String -- UTF-8 characters
UniversalString -- UNICODE code points
BMPString -- UNICODE BMP code points
```

# ASN.1 Simple Types

```
PrintableString -- some printable chars
IA5String -- ASCII characters 0x00..0x7f
ISO646String -- ISO characters 0x00..0xff
T61String
VideotexString
GraphicString -- various charsets
GeneralString -- all registered charsets
CHARACTER STRING
```

# ASN.1 Usage Examples

```
aBarcode BIT STRING ::= '11010001'B
anotherBarcode BIT STRING ::= 'D1'H

barcode OCTET STRING ::= 'D1'H

email IA5String ::= “root@localhost”

foo UTF8String ::= “Пятница!”
```

# ASN.1 Simple Types

```
OBJECT IDENTIFIER -- ISO/ITU OIDs
RELATIVE-OID -- also other OIDs
-- see http://www.oid-info.com/

ObjectDescriptor -- human-readable
```

# ASN.1 Simple Types

```
UTCTime -- time value
-- yyyymmddHHMM[SS][±HHMM]

GeneralizedTime -- time value
-- yyyymmddHHMMSS[.uuu][±HHMM]
```

# ASN.1 Usage Examples

```
sha256 OBJECT IDENTIFIER ::= {
    2 16 840 1 101 3 4 2 1
}

now UTCTime ::= "200103180703Z"

justNow GeneralizedTime ::=
            "20010318090301.456+0200"
```

# ASN.1 Simple Types

```
ANY -- defined elsewhere

ANY DEFINED BY -- + structure ID

INSTANCE OF -- external format

EMBEDDED PDV -- protocol data value
```

# ASN.1 Simple Types

```
Gender ::= ENUMERATED {
    female (1),
    male   (2)
}

Login ::= CHOICE {
    username  UTF8String,
    email     IA5String
}
```

# List vs ENUMERATED vs CHOICE

```
TypeX ::= INTEGER { a (1), b (2) }

TypeY ::= ENUMERATED { a (1), b (2) }

TypeZ ::= CHOICE {
    a INTEGER,
    b NumericString
}
```

# Questions?

# ASN.1 Structured Types

```
Dilemma ::= SEQUENCE {
    egg       EggObject,
    chicken   ChickenObject
}

IPAddress ::= SEQUENCE OF INTEGER
```

# ASN.1 Structured Types

```
Contact ::= SET {
    icqNumber   INTEGER,
    email       IA5String
}

TagList ::= SET OF UTF8String
```

# ASN.1 Keywords

```
… {
    email IA5String OPTIONAL
}

… {
    version INTEGER DEFAULT 3
}
```

# ASN.1 Tagged Types

```
-- Explicit tagging
FullName ::= SEQUENCE {
     firstName   UTF8String,
     nickname    [0] EXPLICIT
                     UTF8String
                     OPTIONAL,
     lastName    UTF8String
}
```

# ASN.1 Tagged Types

```
-- Implicit tagging
LogEntry ::= SEQUENCE {
    message   UTF8String,
    referer   [0] IMPLICIT URL,
    ip        [1] IMPLICIT IPAddress
}
URL ::= SEQUENCE { … }
IPAddress ::= SEQUENCE { … }
```

# Questions?

# Home Tasks

http://courses.cs.ut.ee/2011/appcrypto/Main/Lab05

# May the Force Be with You

Tasks and additional info:

http://courses.cs.ut.ee/2011/appcrypto/Main/Lab05

**Deadline: 2011-03-25 08:00 EET**

Contact: Juri Hudolejev <juri@ut.ee>

Next lab session:

Friday 2011-03-25 **08:30** EET @ Liivi 2 - 205