MTAT.07.017
Applied Cryptography

Introduction, Randomness, PRNG, One-Time Pad, Stream Ciphers

University of Tartu

Spring 2018
Who am I?

Arnis Paršovs

MSc in Cyber Security
Tallinn University of Technology, 2012

Computer Science PhD student at UT
Who are you?

- MSc (Cyber Sec.) - 42
- MSc (Software Eng.) - 10
- MSc (Computer Sci.) - 8
- PhD (Computer Sci.) - 4
- BSc (Computer Sci.) - 3
- MSc Geography - 1
- MSc Physics - 1
- Open University - 1
- MSc (Computer Sci.) - 8
- MSc (Software Eng.) - 10
Crypto courses in UT

- Cryptology I
- Cryptographic protocols
- Cryptology II
- Research seminar in cryptography
- Quantum cryptography
- Topics of mathematics in cryptology
- Applied cryptography
This course

- Practical course
- Learn by implementing
- No proofs – just intuition
Course timeline

16 weeks

- Lecture: Thu 10:15 – 12:00 (room 405)
- Practice: Thu 18:15 – 20:00 (room 206)

6 ECTS – 10 hours weekly

- 2 hours in class
- 8 hours on homework (may vary)
Grading

- Homework every week
- Homeworks give maximum 70% of final grade
  - Bonus points help to achieve the maximum
- Deadlines are strict!
  - Homework deadline – beginning of next lecture
  - May be extended if you have a good excuse
  - Late submission gets 50% of grade
  - Homeworks submitted later than 1 week after the deadline are not accepted
- Exam gives another 30% of final grade
  - Should be easy if you follow the lectures
Programming Environment

Course history:

- 2010: C, C++, Java
- 2011: Java
- 2012: Java
- 2013: Python
- ...
- 2018: Python

Test environment: Ubuntu 16.04.3, Python 2.7.x

Python packages from Ubuntu package repository (not pip)
Homework submission

- Create a private Bitbucket repository and grant me ‘read’ privileges:

- Homework templates will be published at course repository: https://bitbucket.org/appcrypto/2018/

- Feedback will be given using Bitbucket’s code comment feature

- Do not look on homework solutions of others!
  - Plagiarism cases will be handled in accordance with UT Plagiarism Policy
Randomness

- Why do we need randomness in real life?
- Why do we need randomness in crypto?
  - For keys, nonces, etc.
- What is random sequence?
  - Sequence of numbers that does not follow any deterministic pattern
  - None of the numbers can be predicted based on previous numbers
  - Has no description shorter than itself
  - Sequence of bits that cannot be compressed
- Where we can get random numbers?
  - Can we flip a coin to get a random number?
  - Can a computer program generate random numbers?
  - Thermal noise, photoelectric effect, quantum phenomena
Pseudo-Random Number Generator (PRNG)

Deterministic algorithm that produces endless stream of numbers which are indistinguishable from truly random. PRNG is initialized using (hopefully) random 'seed' value.

Linux /dev/urandom implementation:

- Known part of the input does not allow to predict the output
- PRNG is used when true-RNG is not available
- Can be used to “extend” randomness
- Entropy of the output depends on the entropy of the input
Randomness

- Can we tell whether the sequence is random?
  
  ...41592653589...
  3.141592653589793...

  ...000000.......

- Statistical randomness tests
Bits and Bytes

Bit string:
100010000011

$2^{11} + 2^7 + 2^1 + 2^0$

Most significant bit (msb) – left-most bit

Bytes - 8-bit collections (0-255)

Byte - basic addressable element
## ASCII Table

<table>
<thead>
<tr>
<th>Code</th>
<th>Character</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>&lt;NULL&gt;</td>
</tr>
<tr>
<td>1</td>
<td>&lt;SOH&gt;</td>
</tr>
<tr>
<td>2</td>
<td>&lt;STX&gt;</td>
</tr>
<tr>
<td>3</td>
<td>&lt;ETX&gt;</td>
</tr>
<tr>
<td>4</td>
<td>&lt;EOT&gt;</td>
</tr>
<tr>
<td>5</td>
<td>&lt;ENQ&gt;</td>
</tr>
<tr>
<td>6</td>
<td>&lt;ACK&gt;</td>
</tr>
<tr>
<td>7</td>
<td>&lt;BEL&gt;</td>
</tr>
<tr>
<td>8</td>
<td>&lt;BS&gt;</td>
</tr>
<tr>
<td>9</td>
<td>&lt;TAB&gt;</td>
</tr>
<tr>
<td>10</td>
<td>&lt;LF&gt;</td>
</tr>
<tr>
<td>11</td>
<td>&lt;VT&gt;</td>
</tr>
<tr>
<td>12</td>
<td>&lt;FF&gt;</td>
</tr>
<tr>
<td>13</td>
<td>&lt;CR&gt;</td>
</tr>
<tr>
<td>14</td>
<td>&lt;SO&gt;</td>
</tr>
<tr>
<td>15</td>
<td>&lt;SI&gt;</td>
</tr>
<tr>
<td>16</td>
<td>&lt;DLE&gt;</td>
</tr>
<tr>
<td>17</td>
<td>&lt;DC1&gt;</td>
</tr>
<tr>
<td>18</td>
<td>&lt;DC2&gt;</td>
</tr>
<tr>
<td>19</td>
<td>&lt;DC3&gt;</td>
</tr>
<tr>
<td>20</td>
<td>&lt;DC4&gt;</td>
</tr>
<tr>
<td>21</td>
<td>&lt;NAK&gt;</td>
</tr>
<tr>
<td>22</td>
<td>&lt;SYN&gt;</td>
</tr>
<tr>
<td>23</td>
<td>&lt;ETB&gt;</td>
</tr>
<tr>
<td>24</td>
<td>&lt;CAN&gt;</td>
</tr>
<tr>
<td>25</td>
<td>&lt;EM&gt;</td>
</tr>
<tr>
<td>26</td>
<td>&lt;SUB&gt;</td>
</tr>
<tr>
<td>27</td>
<td>&lt;ESC&gt;</td>
</tr>
<tr>
<td>28</td>
<td>&lt;FS&gt;</td>
</tr>
<tr>
<td>29</td>
<td>&lt;GS&gt;</td>
</tr>
<tr>
<td>30</td>
<td>&lt;RS&gt;</td>
</tr>
<tr>
<td>31</td>
<td>&lt;US&gt;</td>
</tr>
<tr>
<td>32</td>
<td>&lt;SPC&gt;</td>
</tr>
<tr>
<td>33</td>
<td>!</td>
</tr>
<tr>
<td>34</td>
<td>&quot;</td>
</tr>
<tr>
<td>35</td>
<td>#</td>
</tr>
<tr>
<td>36</td>
<td>$</td>
</tr>
<tr>
<td>37</td>
<td>%</td>
</tr>
<tr>
<td>38</td>
<td>&amp;</td>
</tr>
<tr>
<td>39</td>
<td>'</td>
</tr>
<tr>
<td>40</td>
<td>(</td>
</tr>
<tr>
<td>41</td>
<td>)</td>
</tr>
<tr>
<td>42</td>
<td>*</td>
</tr>
<tr>
<td>43</td>
<td>+</td>
</tr>
<tr>
<td>44</td>
<td>,</td>
</tr>
<tr>
<td>45</td>
<td>-</td>
</tr>
<tr>
<td>46</td>
<td>.</td>
</tr>
<tr>
<td>47</td>
<td>/</td>
</tr>
<tr>
<td>48</td>
<td>0</td>
</tr>
<tr>
<td>49</td>
<td>1</td>
</tr>
<tr>
<td>50</td>
<td>2</td>
</tr>
<tr>
<td>51</td>
<td>3</td>
</tr>
<tr>
<td>52</td>
<td>4</td>
</tr>
<tr>
<td>53</td>
<td>5</td>
</tr>
<tr>
<td>54</td>
<td>6</td>
</tr>
<tr>
<td>55</td>
<td>7</td>
</tr>
<tr>
<td>56</td>
<td>8</td>
</tr>
<tr>
<td>57</td>
<td>9</td>
</tr>
<tr>
<td>58</td>
<td>;</td>
</tr>
<tr>
<td>59</td>
<td>:</td>
</tr>
<tr>
<td>60</td>
<td>&lt;</td>
</tr>
<tr>
<td>61</td>
<td>=</td>
</tr>
<tr>
<td>62</td>
<td>&gt;</td>
</tr>
<tr>
<td>63</td>
<td>?</td>
</tr>
<tr>
<td>64</td>
<td>@</td>
</tr>
<tr>
<td>96</td>
<td>`</td>
</tr>
<tr>
<td>128</td>
<td>Å</td>
</tr>
<tr>
<td>160</td>
<td>†</td>
</tr>
<tr>
<td>192</td>
<td>ï</td>
</tr>
<tr>
<td>224</td>
<td>÷</td>
</tr>
<tr>
<td>97</td>
<td>a</td>
</tr>
<tr>
<td>130</td>
<td>Ç</td>
</tr>
<tr>
<td>131</td>
<td>É</td>
</tr>
<tr>
<td>132</td>
<td>Ñ</td>
</tr>
<tr>
<td>133</td>
<td>Ö</td>
</tr>
<tr>
<td>134</td>
<td>Ü</td>
</tr>
<tr>
<td>135</td>
<td>á</td>
</tr>
<tr>
<td>136</td>
<td>â</td>
</tr>
<tr>
<td>137</td>
<td>å</td>
</tr>
<tr>
<td>138</td>
<td>ä</td>
</tr>
<tr>
<td>139</td>
<td>à</td>
</tr>
<tr>
<td>140</td>
<td>ã</td>
</tr>
<tr>
<td>141</td>
<td>ç</td>
</tr>
<tr>
<td>142</td>
<td>è</td>
</tr>
<tr>
<td>143</td>
<td>ê</td>
</tr>
<tr>
<td>144</td>
<td>ë</td>
</tr>
<tr>
<td>145</td>
<td>े</td>
</tr>
<tr>
<td>146</td>
<td>ê</td>
</tr>
<tr>
<td>147</td>
<td>î</td>
</tr>
<tr>
<td>148</td>
<td>ì</td>
</tr>
<tr>
<td>149</td>
<td>í</td>
</tr>
<tr>
<td>150</td>
<td>ñ</td>
</tr>
<tr>
<td>151</td>
<td>ô</td>
</tr>
<tr>
<td>152</td>
<td>ò</td>
</tr>
<tr>
<td>153</td>
<td>õ</td>
</tr>
<tr>
<td>154</td>
<td>÷</td>
</tr>
<tr>
<td>155</td>
<td>õ</td>
</tr>
<tr>
<td>156</td>
<td>ú</td>
</tr>
<tr>
<td>157</td>
<td>ü</td>
</tr>
<tr>
<td>158</td>
<td>ý</td>
</tr>
<tr>
<td>159</td>
<td>ü</td>
</tr>
<tr>
<td>161</td>
<td>ø</td>
</tr>
<tr>
<td>165</td>
<td>©</td>
</tr>
<tr>
<td>166</td>
<td>¶</td>
</tr>
<tr>
<td>167</td>
<td>ß</td>
</tr>
<tr>
<td>168</td>
<td>®</td>
</tr>
<tr>
<td>169</td>
<td>©</td>
</tr>
<tr>
<td>170</td>
<td>™</td>
</tr>
<tr>
<td>171</td>
<td>’</td>
</tr>
<tr>
<td>172</td>
<td>“</td>
</tr>
<tr>
<td>173</td>
<td>±</td>
</tr>
<tr>
<td>174</td>
<td>Æ</td>
</tr>
<tr>
<td>175</td>
<td>Ø</td>
</tr>
<tr>
<td>176</td>
<td>∞</td>
</tr>
<tr>
<td>177</td>
<td>–</td>
</tr>
<tr>
<td>178</td>
<td>≤</td>
</tr>
<tr>
<td>179</td>
<td>≥</td>
</tr>
<tr>
<td>180</td>
<td>¥</td>
</tr>
<tr>
<td>181</td>
<td>µ</td>
</tr>
<tr>
<td>184</td>
<td>Ï</td>
</tr>
<tr>
<td>185</td>
<td>ñ</td>
</tr>
<tr>
<td>186</td>
<td>ß</td>
</tr>
<tr>
<td>187</td>
<td>ì</td>
</tr>
<tr>
<td>188</td>
<td>ø</td>
</tr>
<tr>
<td>189</td>
<td>Ω</td>
</tr>
<tr>
<td>190</td>
<td>æ</td>
</tr>
<tr>
<td>191</td>
<td>ø</td>
</tr>
<tr>
<td>200</td>
<td>»</td>
</tr>
<tr>
<td>201</td>
<td>…</td>
</tr>
<tr>
<td>202</td>
<td>✓</td>
</tr>
<tr>
<td>203</td>
<td>À</td>
</tr>
<tr>
<td>204</td>
<td>Â</td>
</tr>
<tr>
<td>205</td>
<td>Ô</td>
</tr>
<tr>
<td>220</td>
<td>‘</td>
</tr>
<tr>
<td>223</td>
<td>fl</td>
</tr>
<tr>
<td>224</td>
<td>÷</td>
</tr>
</tbody>
</table>

Hexadecimal (Base16) Encoding

<table>
<thead>
<tr>
<th>Hex</th>
<th>Value</th>
<th>Binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>'0'</td>
<td>0</td>
<td>0000</td>
</tr>
<tr>
<td>'1'</td>
<td>1</td>
<td>0001</td>
</tr>
<tr>
<td>'2'</td>
<td>2</td>
<td>0010</td>
</tr>
<tr>
<td>'3'</td>
<td>3</td>
<td>0011</td>
</tr>
<tr>
<td>'4'</td>
<td>4</td>
<td>0100</td>
</tr>
<tr>
<td>'5'</td>
<td>5</td>
<td>0101</td>
</tr>
<tr>
<td>'6'</td>
<td>6</td>
<td>0110</td>
</tr>
<tr>
<td>'7'</td>
<td>7</td>
<td>0111</td>
</tr>
<tr>
<td>'8'</td>
<td>8</td>
<td>1000</td>
</tr>
<tr>
<td>'9'</td>
<td>9</td>
<td>1001</td>
</tr>
<tr>
<td>'A'</td>
<td>10</td>
<td>1010</td>
</tr>
<tr>
<td>'B'</td>
<td>11</td>
<td>1011</td>
</tr>
<tr>
<td>'C'</td>
<td>12</td>
<td>1100</td>
</tr>
<tr>
<td>'D'</td>
<td>13</td>
<td>1101</td>
</tr>
<tr>
<td>'E'</td>
<td>14</td>
<td>1110</td>
</tr>
<tr>
<td>'F'</td>
<td>15</td>
<td>1111</td>
</tr>
</tbody>
</table>

- One hex symbol represents 4 bits
- Two hex symbols needed to represent a byte

\[ 2E = 0010 \ 1110 \]
Base64 encoding

bn+ITbj/TRwcSAwT8CZnFZN0me5/AGdFIGNLBLPPo7Nc07T6XTpsTw0QxnM++9xJXKkEEcaEn2Vo9MiAVPVUR5PsFGKZbL7coPRdHD058RokCF4aizWv6+Dqg0lsXsmXliWusn0Q==

- Can represent binary data using printable characters
- Base64 encoded data approximately 33% larger
Bitwise operations

AND:

- extract partion of bit string

\[
\begin{array}{c}
\text{0 0 1 1 1 1 0 0} \\
\text{0 0 0 0 0 1 1 0 (bit mask)} \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\text{0 0 0 0 0 1 0 0 (AND)} \\
\end{array}
\]

OR:

- set specific bits

\[
\begin{array}{c}
\text{0 0 1 1 1 1 0 0} \\
\text{0 0 0 0 0 1 1 0} \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\text{0 0 1 1 1 1 1 0 (OR)} \\
\end{array}
\]

XOR:

- flip specific bits

\[
\begin{array}{c}
\text{0 0 1 1 1 1 0 0} \\
\text{0 0 0 0 0 1 1 0} \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\text{0 0 1 1 1 0 1 0 (XOR)} \\
\end{array}
\]

Shift:

- shift and pad with 0

\[
\begin{array}{c}
\text{0 0 1 1 1 1 0 0} \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\text{0 0 0 0 1 1 1 1 (right shift by two)} \\
\end{array}
\]
Bitwise operations: AND

- Extract bits we are interested in

Example:

```
0 0 1 1 1 1 0 0
0 0 0 0 0 1 1 0 (bit mask)
---------------
0 0 0 0 0 1 0 0 (AND)
```

Python:
```
>>> 60 & 6
4
```
Bitwise operations: OR

- Set specific bits

Example:

```
0 0 1 1 1 1 0 0
0 0 0 0 0 1 1 0
---------------
0 0 1 1 1 1 1 0 (OR)
```

Python:
```
>>> 60 | 6
62
```
Bitwise operations: XOR

- Flip specific bits

Example:

```
0 0 1 1 1 1 0 0
0 0 0 0 0 1 1 0
---------------
0 0 1 1 1 0 1 0 (XOR)
```

Python:

```
>>> 60 ^ 6
58
```
Bitwise operations: Shift

- Shift (right or left) and pad with zeros

Example:

```
0 0 1 1 1 1 0 0
---------------
0 0 0 0 1 1 1 1 1 (right shift by two)
```

Python:

```
>>> 60 >> 2
15
>>> 15 << 1
30
```

- Fast multiplication and division by 2
One-Time Pad (OTP)

- Key generation: key (one-time pad) is random sequence the same length as plaintext
- Encryption operation: XOR ($\oplus$) the key with plaintext
- Decryption operation: XOR ($\oplus$) the key with ciphertext
One-Time Pad (OTP)

Information-theoretically secure (unbreakable), if:

- Key (one-time pad) is truly random
- Key is never reused

\[
\text{plaintext}_1 \oplus \text{key} = \text{ciphertext}_1 \\
\text{plaintext}_2 \oplus \text{key} = \text{ciphertext}_2 \oplus \text{plaintext}_2 = \text{key} \\
\text{key} \oplus \text{ciphertext}_1 = \text{plaintext}_1
\]

- Not used in practice
Stream Cipher

- Key generation: a small key “seeds” the PRNG
- Encryption operation: XOR (⊕) the key with plaintext
- Decryption operation: XOR (⊕) the key with ciphertext

Stream ciphers differ by the PRNG used
- Why is it less secure than one-time pad?
- Encryption on its own does not provide integrity!
- **The same keystream must never be reused!**
Stream Cipher

Solution – on every encryption add unique *nonce* to the key:

- The same *nonce* must never be reused!
- How to generate *nonce*?
  - Counter value
  - Random value
  - Current time
Questions

• Where we can get (true) random numbers?
• Why pseudo-random number is not as good as random number?
• What are the properties of random sequence?
• Can we tell whether the provided sequence is random?
• What happens to data if we XOR it with random data?
• Why brute-force attacks are ineffective in breaking one-time pad?
• Why unbreakable one-time pad is not used in enterprise products?
• How is stream cipher different from one-time pad?
Task: One-Time Pad (OTP)

Implement One-Time Pad cryptosystem.

Encryption should produce a random key file and encrypted output file:

$ chmod +x otp.py
$ ./otp.py encrypt datafile datafile.key datafile.encrypted

Decryption should use the key file and produce decrypted original plaintext file:

$ ./otp.py decrypt datafile.encrypted datafile.key datafile.plain

- Commit “01/otp.py” to your repository
  
  $ git add 01/otp.py
  $ git commit -m "01 homework solution" 01/otp.py
  $ git push
Task: Template

#!/usr/bin/env python
import os, sys  # do not use any other imports/libraries
# took x.y hours (please specify here how much time your solution required)

def encrypt(pfile, kfile, cfile):
    # your implementation here
    pass

def decrypt(cfile, kfile, pfile):
    # your implementation here
    pass

def usage():
    print "Usage:"
    print "encrypt <plaintext file> <output key file> <ciphertext output file>"
    print "decrypt <ciphertext file> <key file> <plaintext output file>"
    sys.exit(1)

if len(sys.argv) != 5:
    usage()
elif sys.argv[1] == 'encrypt':
    encrypt(sys.argv[2], sys.argv[3], sys.argv[4])
elif sys.argv[1] == 'decrypt':
    decrypt(sys.argv[2], sys.argv[3], sys.argv[4])
else:
    usage()
>>> "abraca" + 'dabra'
'abracadabra'

>>> for character in "foo":
...     print "char=%s" % (character)
char=f
char=o
char=o

>>> "abraca"[2:5]
'rac'

>>> "abracadabra".encode('hex')
'6162726163616461627261'

>>> "abracadabra".encode('base64')
'YWJyYWNhZGFicmE=

>>> "abracadabra".encode('base64').decode('base64')
'abracadabra'
Python

Python’s `str` data type can store any byte:

```python
>>> s = 'Abc\x00\x61'
>>> len(s)
5
>>> s[0], s[1], s[2], s[3], s[4] ('A', 'b', 'c', '\x00', 'a')
>>> ord(s[0])
65
>>> chr(65)
'A'
```

- `ord()` can be used to convert byte to integer
- `chr()` can be used to convert integer to byte
Python: Bytes to Integer

```python
>>> s = 'abC'
>>> i = ord(s[0])
>>> i
97
>>> bin(i)
'0b1100001'
>>> i = i << 8
>>> bin(i)
'0b1100001000000000'
>>> i = i | ord(s[1])
>>> bin(i)
'0b1100001011000100'
>>> i = i << 8
>>> bin(i)
'0b110000101100010000000000'
>>> i = i | ord(s[2])
>>> bin(i)
'0b11000010110001001000011'
>>> i
6382147
```

- Convert first byte to integer
- Left-shift integer 8 times
- Convert second byte to integer
- Load second integer in first 8 bits
- ...
Task: One-Time Pad (OTP)

- **Encrypter:**
  - Read the file contents into byte string (e.g., `s = open('file.txt').read()`)
  - Convert plaintext byte string to one big integer
  - Obtain random byte string the same length as plaintext (use `os.urandom()`)
  - Convert random byte string to one big integer
  - XOR plaintext integer and key integer (**please, use this approach**)
  - Save the key (one-time pad) and XOR’ed result (ciphertext) to file:
    - Convert key integer to byte string:
      - Use bit masking and left shift
    - Once more: use bitwise operations!
      - Banned: functions `bin()`, `str()`, `int()`, `bytearray()` and operator `**`!

- **Decrypter:**
  - Perform the operations in reverse order
Task: Test Case

```bash
$ echo -n -e '\x85\xce\xa2\x25' > file.enc
$ hexdump -C file.enc
00000000  85  ce  a2  25          |...%|
$ echo -n -e '\xe4\xac\xe1\x2f' > file.key
$ hexdump -C file.key
00000000  e4  ac  e1  2f          |.../|
$ ./otp.py decrypt file.enc file.key file.plain
$ hexdump -C file.plain
00000000  61  62  43  0a          |abC.|

$ echo -n -e '\x00\x00\x61\x62\x43\x00' > file.plain
$ hexdump -C file.plain
00000000  00  00  61  62  43  00          |..abC.|
$ ./otp.py encrypt file.plain file.key file.enc
$ ./otp.py decrypt file.enc file.key fileorig.plain
$ hexdump -C fileorig.plain
00000000  00  00  61  62  43  00          |..abC.|
```
Please!

• Do not waste your time on input validation
• Do not use imports/libraries that are not explicitly allowed
• Include information of how much time the tasks took (as a comment at the top of your source code)
• Give a feedback about parts that were hard to grasp or implement
• Make a note if something was wrong on slides or you have an idea for improvement
• Do not leave any unrequired debugging output in your solution
• Commit the solution to the main branch of your repository with the filename required

Thank you!