DTTF/NB479: Jouspevdujpo up Dszquphsbqiz

Nbuu Cpvufmm
G-224 y8534
cpvufmm@sptf-ivmnbo.fev

(It should now be obvious whether or not you are in the right classroom…)

CSSE/MA479: Introduction to Cryptography

Matt Boutell
F-224 x8534
boutell@rose-hulman.edu

Agenda: Introductions to…

- The players
- The topic
- The course structure
- The course material

And intro to daily quizzes, worth 10% of grade: Q1

Introductions

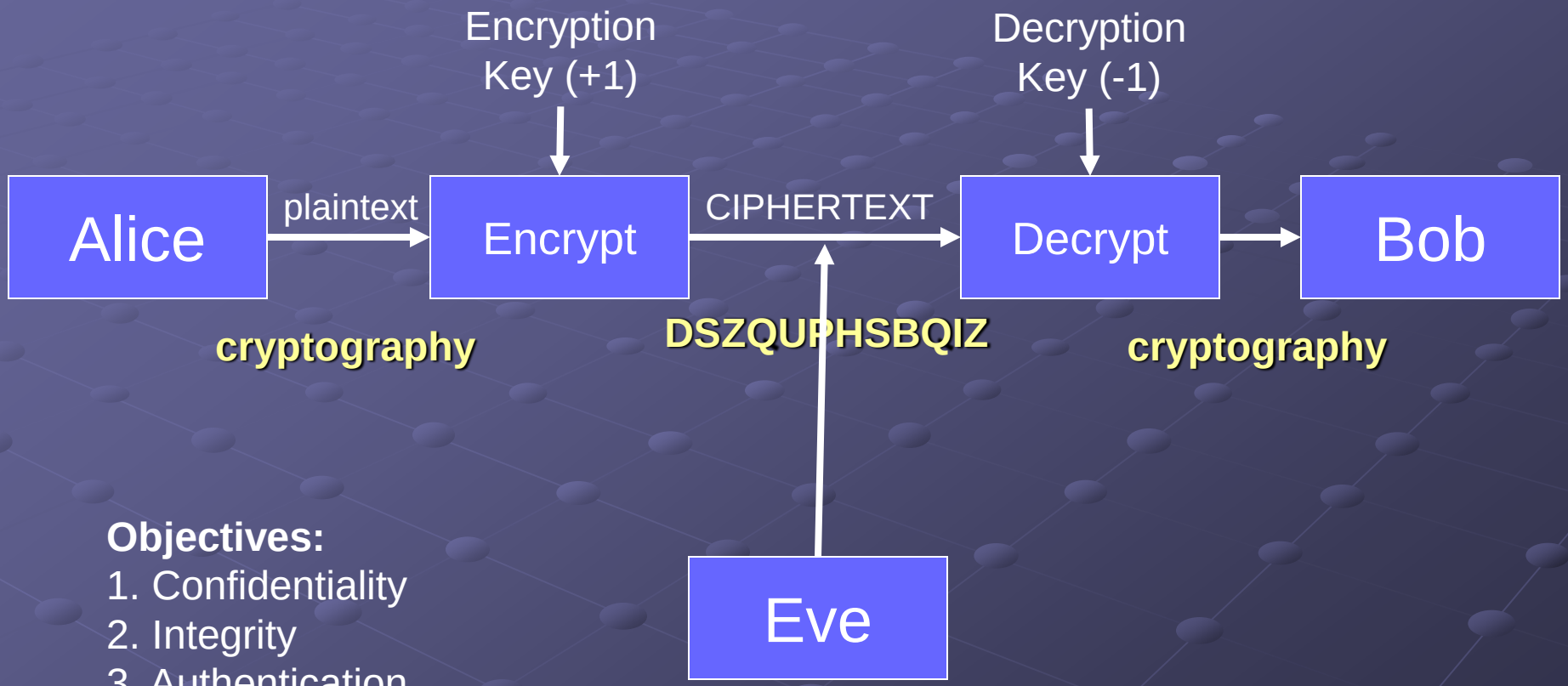
- Roll call:
  - Pronunciations and nicknames
  - Help me learn your names quickly
  - You'll share with classmates on discussion forum
- Me:
  - Sixth year at Rose
  - Taught CSSE120, 120 Robotics, 220, 221, 230, Image Recognition, Fractals, Cryptography, Mechatronics, Robotics senior design

What is Cryptography?

- Designing systems to communicate over non-secure channels

Trappe and Washington, p. 3

Non-secure channels



Objectives:
1. Confidentiality
2. Integrity
3. Authentication
4. Non-repudiation

Trappe and Washington, p. 3

Agenda

- The players
- The topic
- The course structure
- The course material

What will we do?

Learn theory (lecture, text, written problems)

- What would happen if you used *composite* numbers in RSA?

Make and break codes (programming)

- DES Block cipher, classic crypto

Research something new (term project)

- Quantum cryptography, TwoFish, PGP

Admin

- Syllabus
  - Text: highly recommended by students
  - Grading, attendance, academic integrity
  - Angel: Please use the **merged** course:
    - CSSE/MA479 **Spring 10-11** Cryptography
    - The original csse479-01 and ma479-01 are empty
- Schedule
  - Contains links to homeworks (first due Monday)
  - Easy first week…
  - Bookmark in browser:
    - http://www.rose-hulman.edu/class/csse/csse479/201130/
- Email to cssema479-staff for questions

Agenda

- The players
- The topic
- The course structure
- The course material

Shift ciphers

- Attributed to Julius Caesar
- Letters represented as 0-25.
- x → x + k (mod 26)
- **`Cryptography → ETARVQITCRJA`**

- Weak cryptosystem.
  - We learn it to show that “encryption” isn’t useful if it’s not secure.
  - We also use it to study 4 typical attacks to find the decryption key:
    - Ciphertext only (the discussion forums)
    - Known plaintext
    - Chosen plaintext
    - Chosen ciphertext

1. Ciphertext only

Consider *dszquphsbqiz*

```
dszquphsbqiz
etarvqitcrja
fubswrjudskb
gvctxskvetlc
hwduytlwfumd
ixevzumxgvne
jyfwavnyhwof
kzgxbwozixpg
lahycxpajyqh
mbizdyqbkzri
ncjaezrclasj
odkbfasdmbtk
pelcgbtencul
qfmdhcufodvm
rgneidvgpewn
shofjewhqfxo
tipgkfxirgyp
ujqhlgyjshzq
vkrimhzktiar
wlsjnialujbs
xmtkojbmvkct
ynulpkcnwldu
zovmqldoxmev
apwnrmepynfw
bqxosnfqzogx
cryptography
```

- How did you attack the cipher?
- Another trick for long ciphers…

2. Known plaintext

Say I know sample of plaintext *and* corresponding ciphertext.

How long does the sample need to be to find the key?

3. Chosen plaintext

Say I have access to the encryption machine and can choose a sample of plaintext to encode. How can I deduce the key?

Just encode *a*. That gives the encryption key

4. Chosen ciphertext

Say I can choose a sample of ciphertext to decode.

Just decode *A*. How does this give the encryption and decryption keys?

Homework due Monday

- See the schedule page

Affine ciphers

Somewhat stronger since **scale, then shift**:

$x \rightarrow \alpha x + \beta \pmod{26}$

Say y = 5x + 3; x = ‘hellothere’;
Then y = ‘mxggv…’

(Hint: my table mapping the alphabet to 0-25 is really handy)

Affine ciphers: $x \rightarrow \alpha x + b \pmod{26}$

Consider the 4 attacks:

1. How many possibilities must we consider in brute force attack?

Restrictions on α

Consider y= 2x, y = 4x, or y = 13x

The problem is that gcd(α, 26) ~= 1.

The function has no inverse.

Finding the decryption key

- What's the inverse of $y = 5x + 3$?
- In *Integer (mod 26) World*, of course…

Affine ciphers: x → ax + b (mod 26)

- Consider the 4 attacks:
  1. Ciphertext only:
     - How long is brute force?
  2. Known plaintext
     - How many characters do we need?
  3. Chosen plaintext
     - Wow, this is easy.
  4. Chosen ciphertext
     - Could be even easier!