Instructional Toolkit

My Classes | Instructor Tools | Student View | Logout

University of Virginia

Discrete Cryptology
MATH404-1 Fall 2005

Go to another feature (last modified on this date)

Class Assignments

Title	Homework 14
Due date	Dec-5-05 6:00pm
Post from - Post to	not specified - not specified
Required	yes
Electronic submission allowed	no
Late submission accepted	no
Assignment information	

```
- Paper due in class.
- Final exam in class.
- Also turn in:

1. Use Vigenere cipher and codeword "FINAL" to decrypt

FUVDEJZZPCTJYEXBQYLCJICPPFZBNEMMSIYFTTFE

2. I encrypted a message using the RSA cipher with e=7 and n=33
(using the notation from class) and got

16, 24, 29, 22, 26, 29, 9, 24, 5, 39.

However, my private key is weak since n is small.  So break my code
(i.e. find d) and decode my message.
```

Title	Homework 13
Due date	Nov-28-05 6:00pm
Post from - Post to	not specified - not specified
Required	yes
Electronic submission allowed	no
Late submission accepted	no
Assignment information	

```
Problems from Silverman handouts on Toolkit: 9.1, 9.2, 9.4, 10.3,
11.1, 11.2(a), 11.3, 11.8, 16.1, 16.3(a), 17.2

Happy Thanksgiving!
Work on your papers!
```

Title	Homework 12
Due date	Nov-16-05 6:00pm
Post from - Post to	not specified - not specified
Required	yes
Electronic submission allowed	no

Late submission accepted no
Assignment information

```
Section 2.4:  5, 14, 20, 23, 29(a), 31(a), 36-39, 41, 47
Section 2.5:  21(a)(d)(e)
Section 2.6:  1(a)(d)(g), 5, 7, 10, 11, 19, 26, 27
```

Title Homework 11
Due date Nov-7-05 6:00pm
Post from - Post to not specified - not specified
Required yes
Electronic submission allowed no
Late submission accepted no
Assignment information

```
Section 8.2:  5, 6, 18, 19, 21, 25(a)-(d).
Section 8.3:  35, 40, 41.
Section 8.5:  3, 5, 10, 13.
Section 8.7:  1, 5, 7.
```

Title Homework 10
Due date Oct-31-05 6:00pm
Post from - Post to not specified - not specified
Required yes
Electronic submission allowed no
Late submission accepted no
Assignment information

```
Section 7.3:  1, 3, 5, 9(a)(c)(e), 14(a)-(d), 18, 30.
Section 7.5:  3(b)(c)(e), 6, 10, 11, 15, 17, 23, 32, 38, 42(a)(b).
```

Title Homework 9
Due date Oct-24-05 6:00pm
Post from - Post to not specified - not specified
Required yes
Electronic submission allowed no
Late submission accepted no
Assignment information

```
Section 7.1:  4, 6(b)(c)(e), 25, 32(a)(d), 35(a)(d), 38(c), 43, 47.
```

Title Homework 8
Due date Oct-17-05 6:00pm
Post from - Post to not specified - not specified
Required yes
Electronic submission allowed no
Late submission accepted no
Assignment information

```
Section 5.1:  5, 7, 10, 13, 17, 21, 23, 27(a), 33
Section 5.2:  3, 7, 16, 19, 21, 25, 38
Section 5.3:  5, 7

Exam Wednesday, 10/19, covers up to and including Section 5.3.
```

Title Homework 7

Due date Oct-10-05 6:00pm
Post from - Post to not specified - not specified
Required yes
Electronic submission allowed no
Late submission accepted no
Assignment information

```
Section 4.5:  1, 3, 5, 9, 11, 15, 23, 25, 30, 39, 45, 48
```

Title Homework 6
Due date Oct-5-05 6:00pm
Post from - Post to not specified - not specified
Required yes
Electronic submission allowed no
Late submission accepted no
Assignment information

```
Section 4.3:  11, 13, 18, 21, 23, 28, 30
Section 4.4:  5, 6, 10, 15, 19, 24
```

Title Homework 5
Due date Sep-26-05 6:00pm
Post from - Post to not specified - not specified
Required yes
Electronic submission allowed no
Late submission accepted no
Assignment information

```
Section 3.4:  3(b)(d), 5(a)(c)(e), 7, 12, 24, 27(a)(c)
Section 4.1:  3, 8, 15, 21, 25, 32, 39
Section 4.2:  3, 7, 18, 21, 22, 25, 32 (for 21 and 22, see Theorem 3;
for 25, see Example 13)
```

Title Homework 4
Due date Sep-19-05 6:00pm
Post from - Post to not specified - not specified
Required yes
Electronic submission allowed no
Late submission accepted no
Assignment information

```
Section 3.1:  5, 10, 12, 13, 17, 27, 32, 47 (for 27, ok to use the
fact that there are infinitely many primes eventhough we haven't
proved this)
Section 3.2:  3. 10(a)(b)(c)(e)(h), 14, 17, 20, 28, 31, 33, 36-38
(for last three problems, you might want to read
"ExtraordinaryHotel.pdf" on the Materials page also use the result of
exercise 71 in section 1.8)
Section 3.3:  5, 7, 13, 19, 20, 52
```

Title Homework 3
Due date Sep-12-05 6:00pm
Post from - Post to not specified - not specified
Required yes
Electronic submission allowed no

Late submission accepted	no
Assignment information	

```
Section 1.6:  5, 8, 12, 14, 16, 18, 25
Section 1.7:  3, 5, 11, 14, 15, 20, 21, 27, 31, 36
Section 1.8:  7, 12, 15, 17, 21, 26, 32, 35-37, 57, 62

If you missed class Monday, 9/5, please download and read
"ProjectTopics.pdf" from the Materials page on Toolkit.
```

Title	Homework 2
Due date	Sep-5-05 6:00pm
Post from - Post to	not specified - not specified
Required	yes
Electronic submission allowed	no
Late submission accepted	no
Assignment information	

```
Section 1.2:  1, 7(a)(d), 9(a)(d), 15, 20
Section 1.4:  1, 5, 9, 31
Section 1.5:  11, 17, 20, 25, 34, 35, 39
```

Title	Homework 1
Due date	Aug-29-05 6:00pm
Post from - Post to	not specified - not specified
Required	yes
Electronic submission allowed	no
Late submission accepted	no
Assignment information	

```
Section 1.1: 1, 3, 5, 9, 13(a)(c)(e), 17(a)(c)(e), 21, 22, 42
```

Return to previous display assignments page

Top of Page Logout