COMS W4995 Introduction to Cryptography **September 2, 2003**

Lecture 0: LaTeX introduction

Lecturer: Tal Malkin *Scribes: Ariel Elbaz*

Summary

This is an example latex file. You should use this file (`ITC0.tex`) as a template for scribing the lecture notes. Start by modifying the lecture number and details. If you're scribing lecture n, submit your edited file as (`ITC`n`.tex`).

1 Theorems, Proofs, etc.

Definition 1

Theorem 1 *text of a theorem ...*

Proof: starting a proof ... and ending it ■

Claim 2 *text of a claim*

Proof sketch: text of a proof sketch ■

We can also *emphasize parts of the text*

1.1 A subsection on primes

Definition 2 *p is a prime if p is an integer that has no integral factors but itself and 1.*

More examples

Lemma 3 *text of a lemma*

Example 1 *text of an example*

2 Mathematical Equations

Math equations can either be mixed with text,, such as $y = x + 2$ or $2^{2^{13}}$ or $\frac{17!}{2^{34}}$, or else they can be in a sepeate line

$$Pr[x \geq y] \leq \frac{1}{3}$$

or on an automatically numbered equation

$$\{x \ : \ x \leq y \Rightarrow y \geq 0\} \tag{1}$$

We can refer to a specific equation by labelling them. Equation 1 defines the set of values x, such that if x is smaller than y, it must be the case that y is at most 0. Note: you will have to compile the LaTeX file **twice** for equation references to appear correctly.

More advanced equations

$$\begin{aligned} V_{s,0}^{\{q_0,q_1\}} &= V_{s,0}^{\{q_0\}} \cup \ V_{s,1}^{\{q_0\}} \circ \left(V_{1,1}^{\{q_0\}}\right)^* \circ V_{1,0}^{\{q_0\}} \\ V_{s,2}^{\{q_0,q_1\}} &= V_{s,2}^{\{q_0\}} \cup \ V_{s,1}^{\{q_0\}} \circ \left(V_{1,1}^{\{q_0\}}\right)^* \circ V_{1,2}^{\{q_0\}} = V_{s,1}^{\{q_0\}} \circ \left(V_{1,1}^{\{q_0\}}\right)^* \circ V_{1,2}^{\{q_0\}} \end{aligned}$$

3 Itemizing

- First item
- Second item

$\Rightarrow$ You can define the bullet shape that appears to the left.

1. Items can also be numbered
2. And they can be nested
   (a) Just another item.

4 Writing text

The LaTeXcompiler does it's own pagesetting. It converts any number of spaces to a single space, and concatantes sentences to fill the paragraph. You can spread one sentence over as many lines as you want, it will continue as if it was written in a single line. If you want to break a paragraph you need to leave an empty line.

When you want to verify some text not being spread across two lines, e.g. "1 2 3 ... 4 5 6 ... 7 8 9", you can enclose it in `mbox`. LaTeX treats it as a single letter and will never cut it in the middle.

Same text, without `mbox`:
When you want to verify some text not being spread across two lines, e.g. "1 2 3 ... 4 5 6 ... 7 8 9", you can enclose it in `mbox`. LaTeX treats it as a single letter and will never cut it in the middle.

5 Some Symbols

Encryption scheme : $(\mathbf{GEN}, \mathbf{ENC}, \mathbf{DEC})$.

pair : $\langle$a,b$\rangle$

Big O, small o : $k = \mathrm{O}(n), \epsilon = \mathrm{o}(1)$

complexity classes :
$\mathsf{L}, \mathsf{RL}, \mathsf{NL}, \mathsf{P}, \mathsf{NP}, \mathsf{coNP}, \mathsf{RP}, \mathsf{BPP}, \mathsf{ZPP}, \mathsf{coNL}, \mathsf{coRP}, \mathsf{EXP}, \mathsf{PSPACE}, \mathsf{AC}^0, \mathsf{IP}, \mathsf{AM}, \mathsf{coAM}$

Number sets : $\mathbb{N}, \mathbb{R}, \mathbb{Z}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_p, \mathbb{Z}_n, \mathbb{Z}_p^*$

Logical operators : $\wedge, \vee, \neg, \iff, \implies$

Theorem 4 (Fermat's little theorem) *If p is a prime, then for any $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$*

Definition 3 *A function $f\colon \{0,1\}^n \to \{0,1\}^{n+1}$ is a pseudo random generator ...*

> Tal's Note: *If the lecturer feels there are things to be added on some topic, they might appear as a note inside the scribes. This does not necessarily mean that the scribes are not good; Sometimes these notes may refer to topics that are beyond the scope of the course.*