NT-Cryptography MAT4930 *7554* | **Project-Z** | Prof. JLF King *Touch*: 2Jul2018

This optional final-project is due by **noon, Friday, 22Apr2011**, *slid completely under my office door,* LIT402. *Fill-in* every *blank* ⌊.....⌋ on this sheet. Write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed.

For essay questions (**Z2**) *and* (**Z3**), *carefully typeset* (I recommend TEX/LATEX, but others are ok) *a double-or-triple–spaced essay solving the problem. Please start each essay on a new sheet of paper.*

Z1: SHORT ANSWER.

a Alice publishes her ElGamal triple: Modulus $M := 997$, base $G := 174$, and value $V := \langle G^\alpha \rangle_M = 609$, where α is her secret key. (She picks α in $[2\,..\,R)$, where $R = 498$ is the order of the subgp gen. by G.) Bob has a message $s \in [0\,..\,M)$. He picks an ephemeral $\beta \in [1\,..\,R)$, then transmits (C, D) where $C := \langle G^\beta \rangle_M = 88$ and $D := \langle s \cdot V^\beta \rangle_M = 99$. Alice knows that $\alpha = 27$, so she decodes $s =$ ⌊.....⌋.

b Three Jacobi symbols: Two blanks are immed.: $\left(\frac{4203}{2006}\right) =$ ⌊.....⌋. $\left(\frac{4203}{99}\right) =$ ⌊.....⌋. $\left(\frac{120}{27113}\right) =$ ⌊.....⌋.

Z2: Here is part of Hensel's lemma in the singular case. All variables range over the integers.

For a prime q and natnum k, expression "$q^k \bullet\!\!\parallel R$" means that $q^k \bullet\!\!| R$ *and* $q^{k+1} \nmid R$.

I Prove: Lemma 1: *For a prime q and natnum k, suppose $q^k \bullet\!\!\parallel R$. If $S \equiv R \pmod{q^{k+1}}$, then $q^k \bullet\!\!\parallel S$.*

II Prove: Lemma 2: *For intpoly $h()$ and integer $M>0$, necessarily*

$$\forall x,y: \quad [x \equiv_M y] \Rightarrow [h(x) \equiv_M h(y)]\,.$$

III Fix a non-zip intpoly $F()$, a posint T and a prime P. Use $\overset{\ell}{\equiv}$ as a synonym for $\equiv_{P^\ell}$, e.g., $257 \overset{3}{\equiv} 7$ means that $[257 - 7] \bullet\!\!| P^3$. For a ***level*** $\ell \in \mathbb{Z}_+$, an integer $\boldsymbol{\alpha}$ is an "***ℓ-root*** [of F]" if

$$F(\boldsymbol{\alpha}) \overset{\ell}{\equiv} 0\,.$$

Definition. For a level ℓ satisfying

1a: $$\ell \geqslant 1 + 2T\,,$$

say that an integer $\boldsymbol{\alpha}$ is "***ℓ-good***" if

1b: $$F(\boldsymbol{\alpha}) \overset{\ell}{\equiv} 0\,,$$ and the derivative satisfies

1c: $$F'(\boldsymbol{\alpha}) \bullet\!\!| P^T\,.$$

Your overall goal is to prove:

2: Singular-Hensel thm. *Suppose $\boldsymbol{\alpha}$ is ℓ-good. Then there exists a unique $m \in [0\,..\,P)$ such that*

$$\boldsymbol{\beta} := \boldsymbol{\alpha} + mP^{\ell-T}$$

is $[\ell{+}1]$-good. ◊

As a first step, let $\boldsymbol{\beta}_m := \boldsymbol{\alpha} + mP^{\ell-T}$, and use (**??**) to show that each $F'(\boldsymbol{\beta}_m) \bullet\!\!| P^T$.

Similar to the Hensel argument we gave in class, use (**??**) to prove this:

3: Prop'n. *For every integer x and each $m \in [0\,..\,P)$,*

3.1: $$F(x + mP^{\ell-T}) \overset{\ell+1}{\equiv} F(x) + mP^{\ell-T} \cdot F'(x)\,.$$

IV Plug-in $\boldsymbol{\alpha}$ for x in (3.1). Now divide this (by what?), making use of (**??**) and (**??**), and solve for m. Then show that this m is unique in $[0\,..\,P)$.

Finally, carefully verify that *your* $\boldsymbol{\beta}_m$ satisfies all three conditions for being $[\ell{+}1]$-good.

End of Project-Z

	Z1:	___ ___	55pts
Poorly stapled, or missing name or ordinal	**Z2:**	___ ___ ___	135pts
	:	___ ___	−15pts
Not double-spaced:		___ ___	−15pts
	Total:	___ ___ ___	190pts

Please PRINT your name *and* ordinal. *Ta:*

Ord: ⌊.....⌋

HONOR CODE: *"I have neither requested nor received help on this exam other than from my professor."*

Signature: .....

Have a great summer-break, and come back Mathematically refreshed. In Autumn, stop by to say Hi and tell me what you are thinking about.

It was a pleasure working with you this semester.

—"Prof. Jonathan"