Staple!

Team: U

NT-Cryptography MAT4930 *0329* | **Home-U** | Prof. JLF King Wedn., 15Feb2023

Due: ~~Monday, 20Feb.~~ no later than 11:30AM, on Wedn., 22Feb., slid completely under my office door, LIT402.

Fill-in every *blank* on this sheet. This sheet is the *first-page* of your write-up.

U1: Alice publishes her ElGamal *modUlus* $\mathbf{U} := 4094957$, *gen.* $\mathbf{G} := 399510$, and her *public key* $\mathsf{A} := \langle \mathbf{G}^{\alpha} \rangle = 859311$, where α is Alice's private key, and $\langle\cdot\rangle$ means $\langle\cdot\rangle_{\mathbf{U}}$. Bob transmits his public key $\mathsf{B} := \langle \mathbf{G}^{\beta} \rangle = 856746$. Each computes $\boldsymbol{\sigma}=\langle \mathbf{G}^{\alpha\beta} \rangle$, the secret key. Bob skipped class on *known plaintext* day, and erroneously ElGamal's messages $m_0, \ldots, m_9$ to Alice, *but reusing* β. He transmits

$C_0 := 2501615$ $C_1 := 1685151$ $C_2 := 20561$ $C_3 := 2079233$
$C_4 := 2287623$ $C_5 := 2428749$ $C_6 := 990351$ $C_7 := 3630623$
$C_8 := 39151$ $C_9 := 1225900$; *ten ciphertexts* $C_j := \langle \boldsymbol{\sigma} \cdot m_j \rangle$.

Eve knows Bob sent his [crummy] password, $M_K := 11111$, and she tricked him into sending $M_C := 4930$, their Crypto course number. Bob's error, together with the Known and Chosen plaintexts, allow you, Eve, to compute $\boldsymbol{\sigma}=$ ______ and recover all ten plaintexts. Eve used *what* property of M_C that M_K might not possess?

For **b**-bit modulus **U**, with Bob sending N messages [one known, one chosen plaintext], what is the running time $R(\mathbf{b}, N)$ of Eve's algorithm to compute $\boldsymbol{\sigma}$?

U2: RSA uses a modulus N, (en/de)cription exponents E,d so that $\mathsf{E}\cdot\mathsf{d} = 1 + k\varphi(N)$, for some posint k. In class, we restricted Bob's message m to be $\perp N$, then used EFT to conclude that $m^{\mathsf{Ed}} \equiv_N m$.

Pair (m, N) is ***nice*** if: $\forall k \in \mathbb{N}$: $m^{1+k\varphi(N)} \equiv_N m$.
Posint N is ***great*** if (m, N) is nice for *every* integer m.

i Prove that each $N := pq$, with $p<q$ primes, is great.

ii Characterize, with proof, the set of great numbers.

U3: i Use Pollard-ρ to find a nt-factor of $M := 59749$, using seed $s_0 := 7$ and map $f(x) := \langle 1+x^2 \rangle_M$. Make a nice table, labeled

Time	Tortoise	Hare	$s_{2k} - s_k$	GCD(??)

—*but* ***replace*** *the "??" with the correct expression.* You found non-trivial factor $E :=$ ______.

The hare Hits into the tortoise at time $H :=$ ______.

Repeat, showing the table for $s_0 := 24$. Experiment with different seeds; what is the typical running time? [RT means #(f-evals)]. How is it related to the factor you find?

ii A seed s determines a ***tail***; the smallest natnum T for which there is a time $n > T$ with $f^n(s) = f^T(s)$. The smallest such n is $T+L$ where L is the ***period***. Derive (picture+reasoning) a formula for the hitting time $H(T, L)$. [*Hint:* $H(0, L) = L$.]

iii Produce a Floyd-like algorithm that computes both T and L. The number, N, of f-evaluations is upper-bounded by some small constant times $T+L$ (=arclength of ρ). How small can you get $N(T, L)$? [*Hint:* When $T=0$, Floyd's Tortoise-Hare alg. uses $3L$ evaluations.] Your Floyd-like alg. may be able to upper-bnd the f-eval # in form $\alpha T + \beta L$, for specific posints α, β. [Is $T=0$ a special case?]

U4: Bob's RSA modulus is $\mathbf{M} := p \cdot q$, where $p<q$ are **b**-bit primes. Doofusly, Bob wrote value $\mathrm{F} := \varphi(\mathbf{M})$ on a paper napkin, which Eve found. *Describe Eve's algorithm to rapidly compute* p *in time* $\mathsf{O}(\mathbf{b}^n)$, *where* $n =$ ______ $\in \mathbb{Z}_+$.

[Assume, for every k-bit target T, that *sqroot,remainder* $s,r \in \mathbb{N}$ satisfying $[s^2] + r = T < [s+1]^2$, can be found in $\mathsf{O}(k^2)$ time.]

End of Home-U

U1:	___ ___ ___	115pts
U2:	___ ___ ___	115pts
U3:	___ ___	85pts
U4:	___ ___	35pts
Total:	___ ___ ___	350pts

HONOR CODE: *"I have neither requested nor received help on this exam other than from my team-mates and my professor (or his colleague)."* *Name/Signature/Ord*

Ord: ______

Ord: ______

Ord: ______