**EXAM #2A**
**MATH V3025 Making, Breaking Codes**
(D. Goldfeld, 11/21/2017)

NAME: _____, E-mail _____

*Do all of the following problems. Each problem is worth 10 points. Only a simple basic non-graphing calculator is allowed. Please NEATLY write out all answers (with explanations) on these sheets.*

**Problem 1:** Suppose $p$ is a large prime and $\alpha$ is a primitive root (mod $p$). For an integer $m > p^2$, define a hash function $h(m) \equiv \alpha^{5m} \pmod{p}$.

**(a)** Explain how $h$ is pre-image resistant.

**(b)** Show that $h$ is not strongly collision-free by finding a counterexample.

**Answer:**

**Problem 2:** Consider the RSA protocol with $n = 11 \times 17 = 187$. Assume Alice has a secret key $d = 23$ and a public key $e = 7$.

**(a)** Alice computes an RSA digital signature $s$ for the message $M = 2$. What is the signature $s$?

**Answer:**

**(b)** Briefly explain the protocol for verifying the signature $s$.

**Answer:**

**Problem 3:** *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$. The addition law on $E$ is given by:*

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3) = \big(m^2 - x_1 - x_2,\ m(x_1 - x_3) - y_1\big),$$

*where*

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } (x_1 y_1) \neq (x_2, y_2) \\ \frac{3x_1^2 + a}{2y_1} & \text{if } (x_1 y_1) = (x_2, y_2). \end{cases}$$

**(a)** Find all points that are on the elliptic curve $E : y^2 \equiv x^3 + x + 2 \pmod 3$.

**Answer:**

*A point $P$ on $E$ has order $k$ if $kP = \infty$ and $rP \neq \infty$ for any integer $1 \leq r < k$.*

**(b)** Find all points on $E \pmod 3$ that have order 2.

**Answer:**

**Problem 4:** Give an example of a zero knowledge authentication protocol based on the hard problem that it is infeasible to compute square roots (mod $pq$) where $p \equiv q \equiv 3 \pmod 4$ are large primes.

**Answer:**

**Problem 5: (a)** Give the definition of a finite group.

**Answer:**

**(b)** Construct an example of a finite group with 4 elements.

**Answer:**

**Problem 6:**

**(a)** Show that $x^2 + x + 2$ is irreducible over $\mathbb{F}_3$, the finite field of 3 elements.

**Answer:**

**(b)** Consider the finite field of 9 elements consisting of all polynomials in $\mathbb{Z}_3[x] \mod\big(x^2 + x + 2\big)$. Compute $(x + 1)^{-1}$ in this field.

**Answer:**