MATH/CMSC 456 (Washington) Final Exam May 14, 2009

Use 8 pages. Do a separate problem on each page. Write your name on each page. Do not staple.

1. (16 points = 8+8) (a) Let a, b, c, d, e, f be integers mod 26. Consider the following combination of the Hill and affine ciphers: Represent a block of plaintext as a pair (x, y) mod 26. The corresponding ciphertext (u, v) is

$$(\, x \quad y \,) \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (\, e \quad f \,) \equiv (\, u \quad v \,) \pmod{26}.$$

Describe how to carry out a chosen plaintext attack on this system (with the goal of finding the key a, b, c, d, e, f). You should state explicitly what plaintexts you choose and how to recover the key.
(b) Alice is trying to factor $n = 59047$. She notices that $729^2 \equiv 18 \pmod{n}$ and that $42912^2 \equiv 2 \pmod{n}$. How does she use this information to factor n? Describe the steps but do not actually factor n.

2. (12 points = 6+6) Alice uses RSA with $n = 27046456501$ and $e = 3$. Her ciphertext is $c = 1860867$. Eve notices that $c^{14} \equiv 1 \pmod{n}$.
(a) Show that $m^{14} \equiv 1 \pmod{n}$, where m is the plaintext.
(b) Explicitly find an exponent f such that $c^f \equiv m \pmod{n}$ (*Hint:* You do not need to factor n to find f.)

3. (12 points = 6+6) Suppose n is a large odd number. You calculate $2^{(n-1)/2} \equiv k \pmod{n}$, where k is some integer with $k \not\equiv \pm 1 \pmod{n}$.
(a) Suppose $k^2 \not\equiv 1 \pmod{n}$. Explain why this implies that n is not prime.
(b) Suppose $k^2 \equiv 1 \pmod{n}$. Explain how you can use this information to factor n.

4. (8 points) A bank in Chicago wants to send several Gigabytes of data to a bank in Tokyo. They have never had any contact before this. They ask you what they should do. State what cryptosystems they should use and what gets sent using each system. (*Note:* There are several possible answers, but in any case you need two systems to accomplish the task. Do not worry about intruder-in-the-middle attacks or authentication.) (*Another note:* The following is not a solution: "Give me all the account data and I'll personally carry it to them. There's a flight today that connects through Tahiti.")

5. (18 points = 6+6+6) Consider the following signature algorithm. Alice wants to sign a message m. She chooses a large prime p and a primitive root α. She chooses a secret integer a with $\gcd(a, p-1) = 1$ and calculates $\beta \equiv \alpha^a \pmod{p}$. She publishes (p, α, β) but keeps the number a secret. She also has a public hash function h. To sign the message, she does the following:

(1) Chooses a random integer k with $\gcd(k, p-1) = 1$.
(2) Computes $r \equiv \alpha^k \pmod{p}$.
(3) Computes $s \equiv a^{-1}(h(m) - kr) \pmod{p-1}$.
(4) The signed message is (m, r, s).

Bob verifies the signature as follows:

(1) Computes $u_1 \equiv \alpha^{h(m)} \pmod{p}$.
(2) Computes $u_2 \equiv \beta^s r^r \pmod{p}$.
(3) Declares the signature valid if $u_1 \equiv u_2 \pmod{p}$.

(a) Show that if Alice signs the document correctly then the verification congruence holds.
(b) Suppose that Alice uses $k = a$. Describe how Eve can figure out that $k = a$ and show how Eve can compute the value of a. (Note: she might at first have more than one possibility (but probably not very many possibilities) for a; you should include a description of how she determines which is the correct one.)
(c) Suppose the hash function satisfies $h(x) \equiv 2^x \pmod{101}$ and $1 \leq h(x) \leq 100$ for all x. Suppose Eve has a valid signed message (m_0, r_0, s_0) from Alice. Give another message m that Eve can sign with Alice's signature.

6. (14 points = 8+6) (a) Let $p = 11$ and let $m = 5$ be the secret. You want to share a secret among 4 people A, B, C, D so that any three can recover the secret, but no 2 persons can recover it. Explicitly list numbers you could give to each person in order to accomplish this (your answer should have actual numbers, not just letters).
(b) Suppose Person A tries to use only her share to guess the secret. How many possibilities are there for her secret? Explain. (The number of possibilities should be a number from 1 to 11, since the secret is a number mod 11.)

7. (8 points) Suppose Alice signs contracts using a 30-bit hash function h (and h is known to everyone). If m is the contract, then $(m, sig(h(m)))$ is the signed contract (where *sig* is some public signature function). Eve has a file of 2^{20} fraudulent contracts. She finds a file with 2^{20} contracts with valid signatures (by Alice) on them. Describe how Eve can accomplish her goal of putting Alice's signature on at least one fraudulent document.

8. (12 points: 6+6) (a) Eve is trying to find an elliptic curve discrete log: She has points A and B on an elliptic curve E such that $B = kA$ for some k. There are approximately 10^{20} points on E, so assume that $1 \leq k \leq 10^{20}$. She makes two lists and looks for a match. The first list is jA for N randomly chosen values of j. The second is $B - \ell A$ for N randomly chosen values of ℓ. How big should N be so that there is a good chance of a match?
(b) Give a classical (that is, not elliptic curve) version of the procedure in part (a).