Math 195, Section 2
Cryptography
H. W. Lenstra, Jr. (879 Evans, office hours TuTh 2–3 pm, tel. 643-7857, e-mail hwl@math).
Spring 2002, TuTh 11–12:30, 81 Evans.

Take home final.

A-problems. There are three A-problems: A1, A2, and A3. You have to do *all three* of them. Please do them on your own, using no more than the textbook, your class notes, and the material on the web page of the class (address below). Each of the A-problems is worth *five* points.

B-problems. There are eight B-problems: B1–B4 and B5*–B8*. You have to do *three and only three* of them. On each problem that you choose to do, you may cooperate in groups of two or three. However, you should write down the solution in your own words. Do not ask help from people outside the class, and do not show the exam to others. State in your work with whom you cooperated. State also which literature, which web pages, and which computational resources you used. Each B-problem is worth *twelve* points. On each of problems B5*–B8* you can earn a maximum of three bonus points, which may make up for missed homeworks.

Important note. The credit you get for your work will be determined not only by the correctness of your solutions but also by the clarity and conciseness of your exposition.

Grading. Your homework score will be scaled to 50 points, and added to your score on the final. The total score determines your grade for the course.

Web page. The address of the web page for the course is
http://math.berkeley.edu/~jvoight/math195.html

Due date. Put the course number, your name, and your student ID on your work, and hand it in to the instructor no later than Tuesday May 21 at 3:00pm. You may either leave your work with him in 879 Evans, or give it to his secretary, Deborah Craig, in 963 Evans.

Notation. All notation in the problems below is as used in class (see the web page). In particular, $\mathbf{F}_q$ denotes a finite field that has q elements, and $\mathbf{Z}$ is the ring of all integers.

Problem A1. Alice, Bob, Chris, and Eve communicate over a public network. They encrypt all messages they send using the RSA system. Bob and Chris have the same public modulus $n_B = n_C$, but different public encryption exponents: $e_B \neq e_C$.

(a) Show how Bob can decipher all messages sent to Chris.

(b) Suppose that $\gcd(e_B, e_C) = 1$, and that Alice sends the same secret message to Bob and to Chris. Show how Eve can decipher the message.

Problem A2. (a) How many monic irreducible polynomials in $\mathbf{F}_5[X]$ of degree 3 are there?

(b) Give an explicit construction of the field $\mathbf{F}_{125}$.

(c) Pick, in the field that you constructed in (b), an element that does not belong to $\mathbf{F}_5$, and compute its inverse.

Problem A3. Let the elliptic curve E over $\mathbf{F}_2$ be defined by the equation

$$y^2 + y = x^3 + x.$$

(a) List all points of $E(\mathbf{F}_2)$.

(b) Make a table showing $P + Q$ for all P, $Q \in E(\mathbf{F}_2)$. Explain how you made the table. (Avoid performing too many additions.)

(c) How many elements does $E(\mathbf{F}_4)$ have?

Problem B1. This problem is about a monoalphabetic cipher. Throughout, the English alphabet is identified with $\mathbf{Z}/26\mathbf{Z}$ by $A = 0$, $B = 1$, ..., $Y = 24$, $Z = 25$. The encryption function $\varepsilon\colon \mathbf{Z}/26\mathbf{Z} \to \mathbf{Z}/26\mathbf{Z}$ is of the form

$$\varepsilon(x) = \alpha x + \beta \qquad (x \in \mathbf{Z}/26\mathbf{Z})$$

for certain secret numbers α, $\beta \in \mathbf{Z}/26\mathbf{Z}$. For example, if $\alpha = 5$ and $\beta = 9$ then H is encrypted as S, because $H = 7$ and $\varepsilon(7) = 5 \cdot 7 + 9 = 18 = S$.

Suppose now that a very long English plaintext is encrypted by means of the cipher, and that W is the most frequent letter in the ciphertext.

(a) What is probably the third most frequent letter in the ciphertext? (Use the table of letter frequencies from the textbook.)

(b) Suppose next that B is the second most frequent letter in the ciphertext. What are the most likely values for α and β?

(c) Suppose that α, β are as you guessed in (b). Show that to decrypt a ciphertext it suffices to encrypt it twice in succession. (If you guessed wrong in (b) this may be false. In that case, change your guess.)

Problem B2. Let $\mathbf{F}_{256} = \mathbf{F}_2[X]/(X^8 + X^4 + X^3 + X + 1)$, and let $B\colon \mathbf{F}_{256} \to \mathbf{F}_{256}$ be the substitution used by Rijndael (see the class notes on the web page, 04/02/02–04/04/02). Find elements u, $v \in \mathbf{F}_{256}$ with $B(u) = v$ and $B(v) = u$. (You may want to use a computer for this purpose.)

Problem B3. Let $p = 2^{16} + 1 = 65537$. This is a prime number (you do not need to prove this).

(a) What is the order of 3 in the group $\mathbf{F}_p^*$? Is 3 a primitive root modulo p?

(b) What is the order of 2 in the group $\mathbf{F}_p^*$? Prove that $\log_3 2$ is divisible by 2^{11}.

(c) Compute $\log_3 2$. Which method do you use? Show your work.

Problem B4. Analyse the complexity of the Pohlig-Hellman method for computing discrete logarithms (see the class notes on the web page, 04/18/02–04/25/02). More precisely, give upper bounds both for the number of bit operations performed by the algorithm and for the number of operations in the group. These upper bounds should be expressed as functions of the numbers m_1, m_2, ..., m_t that form part of the input. (Do keep the **Important note** on the cover page in mind.)

Problem B5*. Let the *Hamming weight* $W: \mathbf{F}_{256}[Y]/(Y^4+1) \to \{0,1,2,3,4\}$ be as defined in class; that is, if $a = \sum_{i=0}^{3} a_i Y^i \in \mathbf{F}_{256}[Y]/(Y^4+1)$, with $a_i \in \mathbf{F}_{256}$, then $W(a) = \#\{i : a_i \neq 0\}$.

(a) Let $c \in \mathbf{F}_{256}[Y]/(Y^4+1)$ be such that the map

$$M: \mathbf{F}_{256}[Y]/(Y^4+1) \to \mathbf{F}_{256}[Y]/(Y^4+1)$$

defined by $M(a) = c \cdot a$ satisfies $M = M^{-1}$. Prove that there exists $a \in \mathbf{F}_{256}[Y]/(Y^4+1)$, $a \neq 0$, such that $W(a) + W(M(a)) < 5$. (*Note*: if you use the theorem stated about this in class, prove it.)

(b) Discuss the implications of the result of (a) for the design of Rijndael.

Problem B6*. (a) Let r be a prime number, and let n be a positive integer for which $(\mathbf{Z}/n\mathbf{Z})^*$ has an element of order r. Prove: n is divisible by r or by a prime number that is 1 mod r.

(b) Use (a) to prove the following theorem, which was stated without proof in class.
Theorem. *Let r be a prime number, and let k be an integer satisfying $0 < k \leq r$. Then the number $kr+1$ is a prime number if and only if there exists an integer a satisfying $a^k \not\equiv 1 \bmod (kr+1)$ and $a^{kr} \equiv 1 \bmod (kr+1)$.*

Problem B7*. Let $f \in \mathbf{F}_7[X]$ be a cubic polynomial with nonzero discriminant, and let the elliptic curves E_1 and E_2 over $\mathbf{F}_7$ be defined by

$$E_1: \quad y^2 = f(x), \qquad E_2: \quad y^2 = -f(x).$$

(a) Prove: $\#E_1(\mathbf{F}_7) + \#E_2(\mathbf{F}_7) = 16$.
(b) Let $f = X^3 + 4$. Compute $\#E_1(\mathbf{F}_7)$.
(c) Construct an elliptic curve E over $\mathbf{F}_7$ such that $E(\mathbf{F}_7)$ has a point of order 13.

Problem B8*. This is an open-ended problem on Mersenne primes. A *Mersenne number* is a number of the form $2^p - 1$ where p is a prime number, and a *Mersenne prime* is a Mersenne number that is prime.

Investigate what is known about Mersenne primes. In particular: how does one test whether a given Mersenne number is prime? what is the complexity of this method? which are the known Mersenne primes? You may also cover other issues if you like, such as the connection between Mersenne numbers and *perfect* numbers.

Express what you find in your own words, and do not turn in more than three pages.