Cypherpunks know that people have been creating their own privacy for centuries with whispers, envelopes, closed doors, and couriers.

Cypherpunk charter

For here were God knew how many citizens deliberately choosing not to communicate by U.S. Mail. It was not an act of treason, nor possibly even of defiance. But it was a calculated withdrawal, from the life of the Republic, from its machinery.

Thomas Pynchon, The Crying of Lot 49

A Few More Words on Secret Writing

Poe begins “A Few Words on Secret Writing” with a hypothesis about the utility of cryptographic writing: “As we can scarcely imagine a time when there did not exist a necessity, or at least a desire, of transmitting information from one individual to another in such a manner as to elude general comprehension, so we may well suppose the practice of writing in cipher to be of great antiquity” (SW, 114). Today, only a small number of Americans pursue cryptographic security. But as more and more of our social and economic lives are conducted via electronic signals—through e-mail, Net postings, digital bank transactions, and secure corporate communications—the question of privacy, and hence of secret writing, comes to the fore. Among the issues raised by the imminent spread of electronic cryptography, I mention three:

1. **Terrorism.** A prime bogey advanced by opponents of strong public cryptography is the fear that without governmental oversight, terrorists spread over several continents will be able jointly to plan raids like that on the World Trade Center in 1992, with no chance of FBI interception. Partly as a consequence, exporting advanced encrypting technology out of the United States is a felony punishable by a fine of one million dollars and ten years in prison—the same penalty imposed for smuggling nuclear weapons.¹
2. Pornographic delection. Over half the traffic on Usenet newsgroups is allegedly composed of pornographic materials. Not only has anonymous posting produced an enormous number of prurient writers and readers, but the very absence of the body on the Net seems to produce a countervailing imaginative investment in its presence. And in what is already a governmental chestnut used to argue for encryption control, one convicted child molester has used cryptography to hide the identities of his victims.

3. Cyberspace warfare. A computer scientist named Lawrence Detweiler (about whom I will say more) has until recently been furiously battling what he calls the “Medusa phenomenon,” his name for the possibility that one Internet user could fake multiple identities on different networks, located anywhere on the globe. Accessed by modem, these identities could be used in hoaxes that would lead to pitched flame wars enormously destructive of reputations and confidences.

The Net, it seems to say, will be a defining technology for the next two decades. New legal and social protocols will be needed to govern the Net’s global electronic interchanges. Somewhere in the vicinity of sixty million people are now connected to the Internet, with perhaps nine hundred thousand more added monthly—an onslaught of such proportions that John Seabrook compares it to a new tide of internal immigration.

The Internet has also become a fantastic realization of much of what Poe imagined in his essays on cryptography: a matrix for communication whose resonances reach back to the telegraph, through which the world “has become a great nerve, vibrating thousands of miles in a breathless point of time.” And because of the “inherent fluidity of ‘cyberspace,’ where people emerge and submerge frequently,” network identity remains amorphous: instead of the intimate particularity of individual faces and voices, one’s e-mail address consists only of an “arbitrary and cryptic sequences of letters and digits.” In its electronic defiles (which are a series of baffled channels), users can disseminate identities with a freedom that Poe could only imagine. Separated from one’s body, lacking visual or acoustic representation, one’s digital identity is dangerously open to manipulation. Yet the amorphousness of Net identity is also one of its most attractive features, enabling posters and readers of Net communications to gain access to worlds of information that might ordinarily be limited to people of a certain gender, race, profession, or age.

The emergence of an interactive electronic world is already producing legal and social changes related to privacy, identity, and intellectual copyright. Many of these are reminiscent of those tied to the Anglo-American development of commercial print, with newsgroups and World Wide Web pages standing in for the weekly newspapers and coffeehouses that accom-
panyed the print revolution of the eighteenth century. Assistant Secretary of Commerce Larry Irving estimates that the electronic media account for about 15 percent of the gross national product—the same amount as all healthcare industries combined—and that by the millennium, “telecommunications will be America’s foremost export and the world’s No. 1 business.” But how will electronic writing mediate social relations as we enter the age of the Net?

One way to approach this question is to use Poe’s cryptographic writing as a frame. True, in most areas of the Net, Poe is barely present. In a discussion on the alt.suicide newsgroup, someone identified as Joe advanced Poe’s life as evidence that “the mind that is being torn apart produces the greatest works.” He could not, however, actually remember Poe’s name, referring to him only as “the author of ‘Tell-Tale Heart’; I forget his name. His whole life was wrecked.” To which a correspondent replied, “Edgar Allan Poe had a bad life? I didn’t know that. . . . Anyone know more about him? Was he suicidal? How was his life a wreck? Just curious, because I (like most people I guess) have always loved his stuff.”

In other respects, the Internet seems the telos for which Poe’s fictions have been awaiting; indeed, Poe scholars now have a new research tool available, because a group called Internet Wiretap has scanned more than two dozen Poe tales on the Internet that can now be downloaded via anonymous FTP (file transfer protocol). These public-domain texts “include goldbug.poe, mellonta.poe, mystery.poe, purloin.poe, rue.poe, and thouart.poe.” Thou art Poe, indeed. If today we find ourselves in a place shaped by Poe’s cryptographic writing, this has less to do with notions of literary greatness than it does with the way Poe’s writing has participated in the changing historical relationships between literature and technology. “Ride the information superhighway back to its ultimate sources and you end up in the heat and dust of World War II’s secret-code battles,” Julian Dibbel writes, but these battles also require us to reconsider Poe’s writing. To this end, I want to read some recent forms of electronic writing against both Poe’s secret writing and Thomas Pynchon’s Crying of Lot 49, the better to comprehend the contemporary social dynamics of cryptography, particularly in respect to the psychology of encrypting and decrypting. Hence my title: not deciphering the Net (the futility of fantasies of perfect translations is evident), but “ciphering the Net”—subjecting our desires to its electronic graffiti, in which, through the veil of anonymity, we are forced to correspond with our most private selves.

Pretty Good Privacy

Consider the long Net FAQ (for “Frequently Asked Questions”) entitled Identity, Privacy, and Anonymity on the Internet. Its table of contents gives some sense of the giddy world of the telecommuning self, answering ques-
tions about the nature of Net identity, the possibility of privacy, where to learn digital cryptography, and how to become a cypherpunk. If identity cannot be taken for granted on the Net, if it requires special discussion in a FAQ, this is because the posters who can reach millions of readers instantly can also broadcast those messages anonymously by using a form of electronic cipher described as “the most revolutionary new concept in the field since the Renaissance.” These developments are quite recent: even two decades ago, the NSA had a virtual stranglehold on all serious cryptographic research in this country. “That ended abruptly in 1975 when a 31-year-old computer wizard named Whitfield Diffie came up with a new system, called ‘public-key’ cryptography, that hit the world of cyphers with the force of an unshielded nuke.”

Public-key cryptography is a dual-key system, in which every user has both a public and a private algorithm. Although the public key can be distributed without fear of compromising security, the private key “is held more closely than an ATM password.”

For relatively arcane mathematical reasons, a message encoded with either key can be decoded with the other. For instance, if I want to send you a secure letter, I encrypt it with your public key (which I have with your blessing), and send you the cyphertext. You decipher it using your private key. . . . This principle can also be used for authentication. Only one person can encrypt text with my private key—me. If you can decode a message with my public key, you know beyond a doubt that it’s straight from my machine to yours. The message, in essence, bears my digital signature.

Like most cryptographers, Diffie was a math whiz, but from an early age he also had a pressing interest in matters of personal privacy. As a cryptographer coming of age in the early 1970s, he was among the first to profit from Kahn’s magisterial book The Codebreakers, which synthesizes a vast amount of cryptographic lore, setting its technical history within the cultural and psychological context of its deployment. Influenced by Kahn, and working with a Stanford electrical engineer named Martin Hellman, Diffie created a series of algorithms that form the basis of public-key cryptography. Further refined by other mathematicians, the Diffie-Hellman system was eventually marketed under the name RSA Data Security. Despite its imperfections, RSA provided “a working public-key system, and thus did not suffer from the dire flaw of all previous systems: the need to safely exchange private keys.”

The commercial availability of RSA spurred other budding cryptographers, most notably Phil Zimmermann, who developed an alternative system based on Diffie-Hellman known as PGP, for Pretty Good Privacy. An electronic Johnny Appleseed, Zimmermann sacrificed commercial development of PGP, instead placing it free on a computer bulletin board in 1991, where, as he expected, it soon migrated to the Net. “Like thousands
of dandelion seeds blowing in the wind," he wrote, PGP spread through cyberspace. Within hours, people were downloading it all over the country and beyond." As the acronymic forms of strong crypto (that is, public-key cryptography with a key longer than forty bits) multiply, it is not yet clear which will become the standard. But public-key crypto will affect even persons who never use the Net. Many telephone manufacturers are now building cheap automatic encrypting and decrypting devices into their telephones, which have proved so secure that foreign intelligence services have intervened in their design "so that spies can continue to eavesdrop on private conversations." European governments fear "that surveillance operations against drug barons, the criminal underworld and foreign powers could be undermined." According to FBI spokesperson Nestor Michnyak, digital technology is advancing so fast that countersurveillance may be stymied, because the costs of decryption would make widespread eavesdropping prohibitively expensive. Anticipating this, the FBI has proposed amending the Communications Act of 1934 to "require communications service providers and hardware manufacturers to make their systems 'tappable' by providing undetectable 'back doors' through which law enforcement officers could intercept communications." In light of the recent breakthroughs in cryptography and the government's renewed attempts to regulate its use, secret writers have organized a society for the propagation of ciphered privacy. Adapting a term from William Gibson, they call themselves "cypherpunks," and although their battleground may seem remote, the stakes are not: "the outcome of this struggle may determine the amount of freedom our society will grant us in the 21st century." For cypherpunks, the chief value of public-key cryptography "will be to provide anonymity, the right most threatened by a fully digitized society." Currently, by following our electronic footprints, interested parties can "piece together a depressingly detailed profile of who we are: our health records, phone bills, credit histories, arrest records, and electronic mail connect our actions and expressions to our physical selves. Crypto presents the possibility of severing these links." If there is a touch of hyperbole here, it arises because in the future, privacy will likely be an all-or-nothing affair, requiring us to choose between allowing the digital surveillance of our economic and social lives, and making the inviolable crypt of a personal algorithm available to everyone, honest or not. In this context, the United States government's classification of cryptographic algorithms as munitions is no merely technical claim. When a skeptical NASA employee wrote to sci.crypt to ask if strong encryption really belonged in the same category as carrying a loaded gun, Jykri Kuoppala explained that both communication and data storage are shifting to an electronic format, including gun registrations, amateur radio licenses, and criminal registries. Therefore, "using strong cryptography rou-


tinely is being a revolutionary, it is positing oneself directly against the government's important interests of being able to monitor communications.”

Or, as Zimmermann testified to a congressional subcommittee, the growth of digital communications entails “a disturbing erosion of our privacy.”

In the past, if the Government wanted to violate the privacy of ordinary citizens, it had to expend a certain amount of effort to intercept and steam open and read paper mail, and listen to and possibly transcribe spoken telephone conversation. . . . Fortunately for freedom and democracy, this kind of labor-intensive monitoring is not practical on a large scale. Today, electronic mail is gradually replacing conventional paper mail, and is soon to be the norm. . . . Unlike paper mail, e-mail messages are just too easy to intercept and scan for interesting keywords. This can be done easily, routinely, automatically, and undetectably on a grand scale . . . making [an] . . . Orwellian difference to the health of democracy.

Cypherpunks do not merely rely on secrecy to do their work. When the computer scientist John Gilmore obtained a paper written by a cryptographer at Xerox, the publication of which had been quashed by the NSA, he simply posted it to the Net. Within hours it had been distributed both as code and hard copy across the country, and all the bureaucrats at the NSA could not undo Gilmore’s deed. A wealthy former software designer, Gilmore now devotes himself to the cause of electronic freedom, such as in his legal challenge to the NSA for refusing to follow Freedom of Information Act protocols in releasing requested documents. We have returned to familiar ground: the documents in question were forty-year-old declassified manuals written by William Friedman and Lambros Callimahos, which the government later reclassified (shades of the Riverbank Publications!) for unknown reasons. While Gilmore pressed his case against the NSA in court, a friend located copies of two of the documents, one of them on unrestricted microfilm at Boston University. When Gilmore notified the judge hearing the Freedom of Information Act appeal that the documents were already on library shelves, the government informed Gilmore that “distribution of the Friedman texts would violate the Espionage Act.”

The threat to imprison Gilmore for a decade for distributing materials available in the library indicates how seriously the government views its cryptographic monopoly. Only when the San Francisco Examiner publicized the case did the government reconsider its position; two days later, the NSA announced that it had declassified the texts, which were quickly published as Military Cryptanalysis, parts 3 and 4. The irony is palpable: after years spent in the shadows, Friedman’s work has been liberated from the clutches of the NSA by freelance cryptographers inspired by his genius. It is, one might say, Friedman’s posthumous revenge that he has become an avatar to this cryptographic underground, which now poses a greater threat to gov-
ernmental cipher control than the Soviets ever did.\textsuperscript{27} The NSA continues to argue that any publicity about cryptography is injurious to the nation, but Gilmore is skeptical: “We are not asking to threaten the national security. We’re asking to discard a Cold War bureaucratic ideal of national security which is obsolete.” “The decision to literally trade away our privacy,” he adds, ought to be made by the whole society, “not made unilaterally by a military spy agency.”\textsuperscript{28}

In April 1993, the Clinton administration responded to the threat of public-key cryptography by proposing a new system based on an encrypting microchip known as the Clipper. Built into telephones, the chip would provide users with a powerful dual-key encryption program. (A similar chip, code-named “Capstone,” was to be introduced for personal computers.)\textsuperscript{29} In both cases, one key would be unique to the computer or phone; the other would be lodged in a federal repository, administered by a yet-to-be-named government agency. Either key could be used to decipher messages; in the case of suspected criminal wrongdoing, the relevant federal agency would obtain a warrant that would, in turn, be presented to the repository in order to obtain the key to a particular Clipper chip.

Needless to say, cypherpunks find this a case of the fox guarding the chicken coop, particularly because there is no way of knowing whether one’s communications are being monitored. Deluged by attacks from suspicious computer scientists and cryptographers (and lobbied by software firms afraid of losing a $100 million encryption export industry), the government’s National Institute of Standards and Technology backed away from implementation of Clipper and Capstone, only to decide in February 1994 to pursue the chips after all. Soon thereafter, a cryptographer (and cypherpunk) working for AT&T discovered a potentially fatal flaw in the chip’s back door.\textsuperscript{30} Regardless of its ultimate fate, the Clipper chip is the first word in a continuing debate over the rights of citizens to resist governmental oversight of their writing. Since Net traffic statistics indicate a huge demand for anonymous services, it is not even clear that the government has the power to prevent the high-tech encryption of private information. Although some users (particularly scientists) insist that anyone unwilling to identify himself or herself ought to be ignored, other “Netniks” argue fervently for the right and even the necessity of disguise. A “very grateful” Atul Salgaonkar explains that anonymous Usenet discussions helped him resolve “important questions” about his personal life, “due to kind help of other people who had been thru similar situations. In return, I have also replied to anon postings where I thought I could make a positive contribution. . . . Wasting bandwidth is less important than saving lives.”\textsuperscript{31} In \texttt{alt.personals}, or \texttt{alt.sexabuse.rec}, communication is often predicated on the intervening screen of anonymity. Such nameless publication is a constitutive part of American political life; consider Benjamin Franklin’s use of “Silence
Dogood” as an intermediary to express dangerous political opinions. Defending this practice, Stuart Derby explicitly connects anonymous writing to the origins of the United States: “Three of our founding fathers, Madison, Hamilton, and Jay, seemed to think ‘anonymous posting’ was OK. The Federalist papers were originally printed in New York newspapers with authorship attributed to ‘Publius.’ I wonder if you would find their purpose ‘LEGITIMATE?’”

Yet many posters also equate anonymity with direct physical danger: “If I get a phone call from someone who won’t identify himself, I hang up. If I get U.S. mail with no return address, it goes into the garbage unopened. If someone accosts me in the street while wearing a mask, I back away—carefully, and expecting violence. . . . [The psychological] literature is filled with all the various things that people will do anonymously that they won’t otherwise. Including one notorious study involving torture.”

As this text suggests, the issue of cryptographic anonymity is fraught with fears and desires that cannot be explained by the content of a given message. The cypherpunks, for instance, are an exceptionally well-educated and savvy group of activists united around what is arguably the most important First Amendment issue in decades. But there is also something adolescent about their taste for secret writing: much of the attraction of computing derives from a fantasy about the power of hermetic codes.

It will come as no surprise that these fantasies owe a great deal to Poe. Dr. Klaus Pommerening recalls being “impressed by Poe long before I became a professional mathematician.” And as a child, Whitfield Diffie “devoured all the books he could find on the subject of cryptography,” prominently including Poe’s stories. As Levy observes, “certainly there is something about codes—secret rings, intrigue, Hardy Boys mysteries—that appeals to youngsters. Diffie . . . took them very seriously.” Diffie’s pattern holds for hundreds of cryptographers, mathematicians, and software designers: a childhood exposure to cryptographic fiction (either to “The Gold-Bug” proper or to one of Poe’s first- or second-generation imitators), and then a growing interest in the mathematics and psychology of cryptography, often fostered by a sense of superiority over nonciphering peers and teachers. Erich Fromm’s remark seems telling: “The interest in deciphering, as well as in secret codes, may have a great deal to do with a person’s sense of aloneness and isolation and the hope that he might find the related souls with whom he could communicate. The world is closed, and hence he has to decipher what is not meant for him.”

Of the thirty-two responses I received to a query about cryptography and literature on sci.crypt, twenty-eight mention works of cryptographic fiction by name, with those responding often vividly recalling the plot lines decades later. Besides works by Poe, such texts include cipher manuals, children’s fiction such as Alvin’s Secret Code (very often cited), and adult
novels such as Helen McCloy's *Panic*, which was, significantly, a detective story. John Taber remembers that it was "a fine murder mystery based on a mixed-alphabet Vigenere"; after reading it, he "borrowed Gaines' *Elementary Cryptanalysis* from the public library, and taught myself how to solve ciphers." Although Karen Hunt's cryptographic interest was first stimulated by her fifth-grade teacher's math book, that was quickly followed by "kids' books on codes and ciphers and secret writing," and then by ciphers and codes in puzzle books. When a college friend wrote a computer encryption program, Hunt decided to break it "for sport." Remembering cipher types from her old "kiddie books," Hunt recognized it as a Vigenere cipher, which she cracked through a series of educated guesses. "About 2 years later I discovered Gaines' book on cryptanalysis, then Kahn's *The Codebreakers*, then *Cryptologia*, then the ACA (American Cryptogram Association)."

Even more classic is Carl Ellison's recollection that his interest in cryptography was first aroused by Captain Midnight and his decoder ring (actually a belt buckle) which I sent for with Ovaltine labels. It then fell to nothing until I started sending e-mail and needed to encrypt so I invented my own 2 systems (a weak one and a moderate one). Then I started reading about the scientific efforts in WWII and... I got hooked on Enigma—tracked down books on the subject—reread Kahn's *The Codebreakers*—found Deavours' and Kruh's *Machine Cryptography and Modern Cryptanalysis*—read about the Hebern break by William Friedman in 1922 and tried it myself—succeeded—wrote it up for *Cryptologia* and was totally hooked.

Such responses demonstrate the hermetic quality of the world of ciphers: time and again, cypherpunks cite the same progression from children's fiction to magazines to Kahn's *Codebreakers*, Gaines's *Elementary Cryptanalysis*, and the work of William Friedman. As adults, cypherpunks gather around a few small institutions: the American Cryptogram Association (whose membership hovers around seven hundred persons); *Cryptologia* (with a circulation of less than one thousand); and, most recently, the cypherpunks mailing list, whose seven hundred names include those of some of the world's leading cryptanalysts and computer scientists. Cypherpunking represents a return to origins: in light of the NSA's restriction of cryptography, cypherpunks can now do battle with a real secret agency, one whose technological tricks and global reach would have done honor to Ian Fleming's Q or Conan Doyle's Moriarty.

**The Medusa Complex**

In the absence of universal access to public-key cryptography, other strategies have been developed to guarantee the privacy of network writing, most prominently the use of anonymous file servers. Most Net sites employ
addresses that identify a user’s name and institutional affiliation. (When a pseudonym is used, it is a simple matter to finger a poster’s address, querying the Net for public information about a given user.) My Usenet address (Shawn.J.Rosenheim@williams.edu) automatically names both the type of institution (educational) and the specific venue (Williams College) from which my message originates, but “as part of current mailing protocol standards, forging the From: line in messages is a fairly trivial operation” (FAQ, 1.5). Anonymous file servers circumvent this digital trail through the use of a double-blind procedure. One sends a message to the anonymous server, a digital halfway house that scrambles the home address before sending the intact message (now identified as anon.penet.fi, followed by a number) to its intended destination.

The most infamous of these servers was set up in November 1992 by Johan Helsingius (“Julf”) in Finland, using scripts and code written by an American, Carl Kleinpaste. As of January 1993, anon.penet.fi was transmitting a remarkable three thousand anonymous messages daily—about 5 percent of all postings on the Usenet (FAQ, 8.4). Such “immense popularity” is due, Detwiler speculates, to “the capability for ‘global’ anonymity which has allowed users to find creative uses in diverse areas not previously envisioned.” But when coupled with Julf’s “total commitment to preservation of anonymity,” such creativity can do real damage. In 1993, “commotion ensued” when an anonymous user “posted a supposed transcript of desperate crew dialogue during the Challenger shuttle disaster via anon.penet.fi to sci.astro. Although the transcript had been posted in the same place a year earlier (then non-anonymously) and actually originated not with the poster but a New York news tabloid, subsequent responses consisted largely of outrage at the poster’s use of anonymity.” As the original poster later conceded, the story “‘seemed likely to have been fabricated,’ suggesting . . . that the original intent was not to provoke outrage but gauge reactions on the authenticity of the story (albeit crudely), free of personal risk from perceived association with the item” (ibid.).

In the face of the bitter criticism that followed this incident, Julf was subjected to “extraordinary pressure to dismantle his server.” Because he would not do so, the Finland server crashed as a result of a “saturation mail-bombing” initiated by an anonymous user. To his dismay, Julf learned that Kleinpaste had written his code more as a programming experiment than as a tool for unimpeded free expression; when Julf used this code to extend unrestricted anonymity, he offended Kleinpaste’s sense of propriety, as if anonymity violated the social compact needed for true conversation. Kleinpaste retaliated with a series of abusive postings, in which, after calling Julf a “rude bastard,” he regretted his part in creating the server. Although Kleinpaste did not copyright the code, he said “I thought that some concept of politeness and good sense might follow it to new homes. Interesting that
Johan’s ideas of politeness and good sense seem to have nearly no intersection with mine. I could even cope with universal anon access if Johan would engage in abuse control, but that seems to be outside the range of reality.”

A “sad and upset” Helsingius rather disingenuously replied that although he had intended to provide the service only to Scandinavian users, many people had asked him to open the service to the international community. “I now realize that I ought to have contacted you at that point to ask how you feel about me using your stuff in such a context. Again, I really want to apologise. And I will replace the remaining few pieces of code that still stem from your system. Unfortunately there is no way to remove the ideas and structure I got from you.”

Unable to control Julf’s server, a “seriously rude” Kleinpaste considered using the digital equivalent to capital punishment. Reasoning that Julf “didn’t ask the greater Usenet whether universal anon access was a good idea; he just did it,” Kleinpaste contemplated retaliating by programming the server to cancel all anonymous postings, a prospect that filled him with a Strangelovean fervor:

I think I’ll arm the Usenet Death Penalty, slightly modified, not for strategic whole-site attack, but tactical assault. . . . In fact, I have 8 people who have expressed privately the desire and ability to arm the UDP. P.S. No, in fact there are not 8 newsadmins ready to arm the UDP. It would be amusing to know how many people gulped hard when they read that, though. . . . P.P.S. Now that I’ve calmed some fears by the above P.S. . . . There are 2 newsadmins ready to arm the UDP. They’ve asked for my code. I haven’t sent it yet. Only one site would be necessary to bring anon.penet.ji to a screeching halt.

The exchange between Kleinpaste and Julf manifests deep confusion in the way each thinks about how writing is attributed. For Kleinpaste, universal anonymous service would turn the Net into a speaking mirror, in which the disembodied messages on his monitor would take on the dimensions of paranoid projection. Julf responded by threatening to expose the attacker’s identity—just what the server was designed to protect: “As we are talking threats here, let me make one as well. If somebody uses something like the UDP or maliciously brings down anon.penet.ji by some other means, it will stay down. But I will let the users know why. And name the person who did it. OK? As somebody said on this thread: ‘You have to take personal responsibility for your actions,’ right?” Kleinpaste—whose attacks continually invoke notions of politeness—finds that the prospect of unimpeded anonymity incites in him an incivility so extreme that it leads to fantasies of digital death. Meanwhile Julf, the advocate of privacy, responds to the anonymous attack on his server by threatening the assailant with exposure, all the while remarking piously on the importance of personal responsibility on the Net. As with the Challenger posting that only became inflamma-
tory once its source was effaced, the threat posed by cryptography clearly has less to do with the incendiary content of the messages than it does with the anxiety produced by their lack of a signature.

The reverse side of such paranoia is narcissistic identification. Earlier I called Poe’s ciphered self-correspondence billets-doux to himself, and the cryptographic anonymity of the Net also facilitates a kind of love letter. Consider the series of postings to someone identified only as Anne: “You don’t know me,” the first letter begins; “I don’t really know how to say this but I’ll give it my best shot. I’ve been watching you for a long time now and I’ve always wanted to go up to you and say hi. I nearly did a number of times but my courage failed me. . . . There’s something about you that just keeps me back.” In their paratactic sincerity, these notes offer no threat to the correspondence of Abelard and Heloise: “I saw you the first time at Learned. You were wearing a denim jacket and you sat down next to me. My God, I couldn’t keep my eyes off you! I just thought you were the most beautiful woman in the room. You have a truly classic face and I must admit that your square jaw is a turn-on! Anyway, I knew immediately that you were somebody special, smart and beautiful. (This is going to sound really corny and I’m already getting embarrassed) I knew that you were the woman for me.” Even after encouragement, the anonymous sender was still too shy to meet Anne face-to-face: “I’m not used to pouring out my feelings to a total stranger so I’m sitting here flushing as I type. I don’t know if I can introduce myself to you right yet (scaredy cat!) so I guess you’ll have to live with the mystery a little longer.” Eventually a meeting was arranged, after which Anne and her beau discussed their impressions via e-mail: “I didn’t think our meeting would go as well as it did. I had visions of us standing and staring at each other, wondering what the hell to say. Whew! Thank God for M*A*S*H, huh?” Anne’s correspondent remarks on the oddness of meeting in the flesh, of seeing and being seen: “It feels a little weird writing to you now that you actually know who I am. But I kinda like the feeling of being anonymous and yet not. . . . Makes no sense, does it? Guess I find it easier to write down my feelings rather than say it straight to your face.”

The kicker to this romance is that, as we learn in a header to the posting, “Anne” is a pseudonym, and her correspondent is none other than Anne herself, who explains: “About two years ago, I was bored at work so I started emailing love letters to myself. Still, it’s got an interesting storyline that has come true since then! . . . I have no problem with people emailing my stuff around, as long as my name remains with it. BTW [by the way], Anne is not my name.” What can be so delightful as a secret intercourse? Anne—an electronic Narcissa—sees herself reflected as the other in the digital mirror of the Net. “By treating his image as if it were another person even though he knows it is not,” Narcissus reveals that “if the self is at once both a cause and a function of self-consciousness . . . then the origin of
the self is a union that differentiates, a coming together to hold apart.”47 By condensing the exchange of love letters into a secret auto-correspondence, Anne reveals the narcissism of cryptographic writing, mediating her desire through the Net’s electronic alterity. In his preface to “Marginalia,” Poe almost anticipates the charms of such alienation when he indulges in the fantasy that the marginal comments in his own texts might have been written by another person. (As Stephen Rachman demonstrates, Poe’s elaborate fiction of detailed marginal notes affixed to his favorite works with gum tragacanth does not at all correspond to the truth, which is that Poe’s tiny library was largely unmarked.)48 But if Net postings necessarily return to one’s screen alienated by their electronic circuit, such alienation seems to be a prerequisite to a new narcissism: Anne’s strategy requires her not only to write to herself as another, but to post both halves of her correspondence to the world (meanwhile insisting that her pseudonym remain attached to her letters), as she rounds the orbit of her desire.49

To understand the reciprocal hostility and desire aroused by anonymity, I want to consider an earlier hoax, which, like the Challenger controversy, also involved interplanetary travel and a New York tabloid. In 1836 Richard Adams Locke, editor of the New York Sun, published an article “announcing very remarkable astronomical discoveries made at the Cape of Good Hope by Sir John Herschell,” received by the Sun “from an early copy of the Edinburgh Journal of Science” (“The Literati of New York,” PT, 1221). In the articles that followed, readers were treated to the description of the casting and assembly of an enormous new telescope, which enabled Herschell and Sir David Brewster (he of the Maelzel’s Chess-Player expose) to perceive the fauna of the moon, right down to the hairy veil protecting the eyes of moon-bison from the sun’s rays. Poe concludes: “From the epoch of the hoax The Sun shone with unmitigated splendor. The start thus given the paper insured it a triumph; it has now a daily circulation of not far from fifty thousand copies, and is, therefore, probably, the most really influential journal of its kind in the world” (ibid.)

Calling this invention of the penny press “one of the most important steps ever yet taken in the pathway of human progress” (ibid.), Poe sought with “The Balloon-Hoax” to imitate Locke’s success. Poe writes: “The Atlantic has been actually crossed in a Balloon!”: “Astounding News by Express, via Norfolk!—The Atlantic Crossed in Three Days! Signal Triumph of Mr. Monck Mason’s Flying Machine! . . . The subjoined jeu d’esprit . . . was originally published, as matter of fact, in the New-York Sun, a daily newspaper . . . The rush for the ‘sole paper which had the news,’ was something beyond even the prodigious.” Copying Locke’s moon hoax, Poe provides ample verisimilar detail pertaining to the balloon’s design and propulsion (it was driven by means of an Archimedian screw), with the particulars “copied verbatim from the joint diaries of Mr. Monck Mason and Mr. Har-
rison Ainsworth” (“The Balloon-Hoax,” PT, 743-44). As in the Challenger story, there is a link between a New York tabloid and flight, in a hoax whose explosive force derives from its anonymity as Poe seizes on the potential for the new medium to galvanize—or fool—an enormous readership.

Through such hoaxes, Poe exploded the protocol used in reading the nascent penny press, to the intended delight of its readership. Poe also satirized the incoherent anonymity of the printed word (produced as much by the vagaries of market production as by the technical incompetence of printers) in stories like “X-ing a Paragrap,” setting its typographical chaos against Dupin’s sophisticated scheme for revenge in “The Purloined Letter,” which depends for its success on Minister D——’s close acquaintance with Dupin’s manuscript (or “hand”).50 Poe’s concern with locating the writer’s person in the work also finds expression in his insistence on the indexical relation between self and script, as in his pair of articles on autography.51 Handwriting analysis permits readers to interpret a given author in light of the clues given in his or her script, as when the chirographic “scorn of superfluous embellishment” by Professor Charles Anthon also distinguishes his literary compilations, or when a Washington Irving grown “slovenly in the pursuit of his literary tasks” finds that such slovenliness “has also affected his handwriting” (CW, 2:283, 272).

Save for autography and anastatic printing (an early form of xerography), which represent his last-ditch efforts to tie writing to the body (an obliquely hieroglyphic dream), Poe accepted and sought to profit from the anonymity of mass publication. The most interesting of these attempts is that represented by his (probable) pose as “Outis,” the “no one” whose charges of plagiarism against Longfellow ignited the Little Longfellow War, and whose anonymity is still producing a modest immortality for its uncertain author.52 According to Meredith McGill, Poe “bitterly attacked the use of anonymity in criticism, as when he complained of the quarterlies: ‘Who writes?—who causes to be written? Who but an ass will put faith in tirades which may be the result of personality hostility, or in panegyrics which . . . may be laid, directly or indirectly, to the charge of the author himself?’ (ER, 1009).”53 But Poe’s double-edged conclusion seems to be that given the system of anonymous review, writing may always hide vested interests. Poe exploited this in his puff for “The Literary Life of Thingum-bob,” which appeared unsigned in the Southern Literary Messenger. Aiming to ride the buzz created by the story’s anonymous appearance, an unnamed Poe asked in the New York Evening Mirror: “The question is put to us, especially, here in the North,—‘who wrote it?’ Who did?—can any one tell?”54

In this light, the prominently physiognomic qualities of Internet language seem like attempts to forestall equivalent sorts of manipulation today. Just as Poe insisted on chirography, many people have a powerful desire to make the cryptograph stand in metonymic relation to its author, connect-
ing the digit to the digital. Metaphors of hands proliferate. In addition to *fingering*, there are many related terms. In the world of virtual reality, one relies on *data-gloves*; although the *digital signature* produced by public-key systems is inviolable, RSA cryptographers have developed an additional digital code known as a *fingerprint*: a secure 128-bit message digest algorithm, or cryptographic hash, of the plaintext. Levy suggests that the cypherpunks hope to erase "an individual's informational footprints," and Graham Toal (*gtoal@gtoal.com*) speaks of identifying the stylistic *fingerprint* of an anonymous poster whom he hopes to flush. (Similarly, James Phinney Baxter refers to Folio evidence for Baconian authorship as the latter's *thumb marks*.)

Not only does this complex of metaphors return us to Adamic fantasies of self-reflecting language, but as the regulatory origins of fingerprinting reveal, there is considerable state investment in the proper attribution of writing—a desire allegorized in the crisis produced by the sight of an unknown footprint in *Robinson Crusoe*. In response, Net readers sometimes turn to stylistic analysis, as cryptography doubles back on literature. A posting by Paul Leyland on *sci.crypt* suggests solving problems of attribution by investigating the writer's idiosyncratic prose: "An author's style tends to be quite characteristic: the mean and variance of words per sentence, and letters per word; the incidence of spelling and grammatical errors, both in type and number. The number of adjectives; the size of vocabulary; distribution of punctuation (I tend to like semicolons and parenthetical remarks, for instance). There are many such characteristics." Although such identifications may not be made "to universal agreement," Leyland authorizes such analysis by noting that "these methods have been used to identify rediscovered poems by Shakespeare." Where once the text of Shakespeare spurred readers to (spurious) cryptographic discoveries, now questions of electronic anonymity are resolved through techniques for identifying literary provenance.

Anxiety about the uses of anonymity is probably not misplaced. Besides the lurid dangers linked to it by the NSA (terrorism, international drug cartels, child pornography, pandemic tax fraud), anonymity also carries psychic and political costs. In his novel *Ender's Game*, Orson Scott Card imagines a world in which the anonymity of the Net provides a new forum for political manipulation. Two brilliant children realize that "with false names, on the right nets, they could be anybody. Old men, middle-aged women, anybody, as long as they were careful about the way that they wrote. All that anyone would see were their words, their ideas. Every citizen started equal, on the nets." Hiding behind forged identities, they conduct a series of debates that influence foreign policy: "Valentine would prepare an opening statement, and Peter would invent a throwaway name to answer her. His answer would be intelligent, and the debate would be lively. . . . Then they
would enter the debate into the network, separated by a reasonable amount of time, as if they were actually making them up on the spot” (96).

As in fiction, so in life: Card’s novel has provided the direct model for a dramatic contest over the nature of cryptographic anonymity. On one side is Lawrence Detweiler, author of the sober *Identity, Privacy, and Anonymity FAQ*, whose fear of Medusan “pseudospoofing,” or network posting under multiple identities, has taken spectacularly paranoid form. In “the most treacherous and evil” scenario, Detweiler wonders: what if Medusa “was actually Satan in disguise”? Suppose further that she liked to

“punish” people with her “tentacles” whenever they “misbehaved,” by resisting her oppression. She could be quite unpleasant, don’t you think? She could consistently flame their arguments from different tentacles, even if the posts were intelligent, just out of spite. . . . She might have all her sisters try to work on the person in particular and break them down. “You are not going to have any friends if you keep this up. Why are you such a troublemaker, anyway?” Or, if the person has recognized the brainwashing and is amidst flight, she could try to lead him back to darkness. “Oh, I so enjoyed your posts, please reconsider.” This from a tentacle the victim has never heard from before.61

In late 1993 Detweiler became convinced that a number of well-known cypherpunks were really aspects of a retired Intel physicist named Tim May, who, as one of the principal architects of the cypherpunks, and as the author of the “Crypto Anarchist Manifesto,” was at the center of a potent cryptographic plot. With its welter of assertions and counterassertions, forged identities, and evasive replies, the flame war that ensued is far too complex to summarize easily. But the following excerpts do convey the dynamics of secrecy, revelation, and role playing galvanized by anonymity. I begin in midwar, with Detweiler’s attack on a “Mr. Brandt,” who, he imagines, is part of a cypherpunk cabal dedicated to the “art, science, and religion of deceiving others on the Internet and in the media.” Asking “Are you an ‘insider,’ Mr. Brandt?” Detweiler goes on to deny Brandt’s independent existence: “If anyone would like to entertain themselves by determining whether he is a tentacle, a Medusa Sister, or Medusa herself, send him e-mail. Speaking from experience built up over many weeks on ‘cyberspatial exorcisms,’ I would be willing to wager cash that you will not be able to associate him with an actual human being.”62

In fact, Detweiler alleges, several of his correspondents failed to provide direct testimony about their solo identities. Tim May, he claims, “refused to state a simple sentence to me in the form ‘I have never posted under the name J. Dinkelacker.’” Later that day, however, an exasperated May posted to the Net, explicitly denying this: “I’m not ‘Jamie Dinkelacker’ or ‘Hal Finney’ or ‘Eli Brandt’ or ‘Nick Szabo’ or any of the other dozen or so
folks Detweiler routinely rants about me being. Argghh! What more can I say to this raving lunatic?"  

May mustered abundant circumstantial detail pertaining to his existence, including his phone number, and nearly a dozen other people responded in his support, among them Perry Metzger, who observed that Nick Szabo lived in Cupertino, Tim May in Aptos, and Eric Hughes in Berkeley. Further, “all of them have been seen at the same place at the same time in public—for instance, by over 100 people at the Extropy Magazine 5th Anniversary Party, at Cypherpunks meetings, etc. I can personally verify that all of them exist and are separate people.” To prove his own identity, Metzger listed information about his job at Lehman Brothers in New York, his presence in corporate filings, and his telephone number, adding that “anyone who wants to call Tim and call me can easily verify that at the very least we have different voices.”

“In any case,” Metzger wrote to Detweiler, turning the tables, “the ‘Medusa’ is you. You have disrupted lots of people’s lives—you’ve mailed death threats to dozens of people, ‘pseudospoofed’ as at least a half dozen aliases using an12070@anon penet fi, and wrecked mailing lists.” Apparent­ently Detweiler—who stands accused of posting as “an12070, The Executioner, S. Boxx, The Pervert, The Psychopunk, and such pseudonyms”—is a victim of the psychic reversibility that accompanies the cryptographic imagination: as L. Detweiler, enemy of anonymity, and as hit-and-run poster an12070, Detweiler echoes Angleton’s fascination with moles, Dupin’s with Minister D——, and Poe’s self-hoaxing publications as “Walter G. Bowen” and “Outis.” In the face of cypherpunk disinformation, Detweiler (who denied any relation to “the paranoid ranter and conspiracy theorist an12070”) began reposting other people’s messages with derisive commentary. As he wrote in response to May:

Poor deluded Larry takes any such efforts to resolve his delusion as further proof of the Grand Conspiracy to drive him crazier than he already is.

Yes, I am quite insane.

What a strange world the Net is becoming.

No thanks to you.

—Tim May, a Real Person

Owner of many tentacles. Please list all the sites you have ever posted from, Mr. May. Ooops, that would be an Orwellian Invasion of your privacy. A McCarthyist Inquisition. Hee, hee. You cryptoanarchists are so silly. I am having great fun using your techniques of cyberspatial warfare against yourselves. I will not relent until top leadership issues unequivocal statements on
your involvement and knowledge of pseudospoofing. . . . I await the fireworks!  

Should one think Detweiler’s game of radical skepticism merely creepy fun, it is worth contemplating that I was unable to prove who, exactly, Detweiler was. When I called Tim May at the number listed in his Net signature, I reached a curiously circular telephone answering machine, which said that since the machine was unreliable, it was best not to expect a reply to any message, but to call again. I called Perry Metzger at the number in his Net address, but heard what claimed to be Metzger’s recorded voice tell me that he had resigned from Lehman Brothers. The voice, which added that I should hold on if I needed assistance, then disconnected. I tried to reach Detweiler at Colorado State University, the originating address of his postings, but could not find him in the school’s directory of faculty, graduate students, or undergraduates. No one I reached in the computer science department had heard of him. A telephone directory search of Fort Collins turned up a “Lauren Detweiler,” but he turned out to be a retiree who listened patiently to my questions and then said, “Now what’s this about writing?” He had never, he informed me, used a computer, nor did he have any relatives in the area.

Here I briefly halted, unwilling to interrupt a delicious sense, half pleasure and half terror, at finding the world of certainty recede into conspiracies of undetermined shape or purpose. Apparently, the facts by which May and Metzger hoped to authenticate themselves—jobs, phone numbers, answering machines—are as easily suborned as Detweiler fears: “The truth is,” he explains,  

that every attempt I have made to verify certain identities has failed and led only to more grisly conclusions, such as that Cypherpunks have gone to the length of registering NIC [Network Interface Control] domains and buying out-of-state phone numbers. Do not tell me this is impossible! A businessman friend of mine has a local phone number in NY that forwards to Denver! Cypherpunks could use this very readily! (My kingdom goes to anyone who can provide me with the ability to trace the ultimate destination of phone calls in this way, and help uncover the amazing extent of the Cryptoanarchist conspiracy!)  

In thinking about the Detweiler-cypherpunk flame war, I came up with five possibilities, all of which seemed plausible, but none of which I could prove:  

1. In his defense of network responsibility, Detweiler went mad, letting the debate over anonymity devolve into a full-blown psychotic battle with invisible enemies. (Detweiler as a psychological victim of anonymous electronic writing.)
2. In a cruel and weirdly sustained prank, unknown enemies of Detweiler’s forged his signature and sent out hundreds of unauthorized messages designed to defame him and to muddy the waters of a crucial First Amendment debate. (Detweiler as a victim of anonymous electronic writing practiced by others.)

3. Terrified at the prospect of losing control over its ability to eavesdrop electronically, the NSA hired or invented “L. Detweiler” to sow confusion among the most prominent group of cryptoanarchists and to undermine support for anonymity. Think of this as the high-tech version of FBI infiltration of the Students for a Democratic Society. (Detweiler as an agent provocateur in the pay of an evil government.)

4. Detweiler posted all the messages attributed to him, fully cognizant of their outrageous and contradictory character, in order to demonstrate how the unrestricted use of anonymity could lead to social chaos and personal injury. (Detweiler as a meta-Medusa, polemically making a point about anonymity.)

5. “Detweiler” is an invented Net persona, created for purposes unknown. (The scariest prospect of all.)

Frustrated and confused, I telephoned Tim May again late one night. This time someone answering to his name picked up after two rings, and confirmed my hunch that the fourth hypothesis was the closest to the truth, although even that can hardly explain the weirdness of the affair. According to May, Detweiler is a precocious recent graduate in computer science of Colorado State University who had become fascinated by cryptographic anonymity. In the spring of 1993, Detweiler asked to be put on the cypherpunks mailing list, but when some of his ideas (including one for an “electocracy,” an electronic democracy that would poll citizens to determine social policy) were treated with insufficient respect, he began posting messages excoriating members. In a turnabout from the moderation of his FAQ, Detweiler has especially come to disdain the notion of unlimited anonymity. Not content with argumentation, he seems rather cleverly to have performatively demonstrated the risks of anonymity. Borrowing from Ender’s Game, Detweiler began generating alternate identities (including my favorite, “Jim Riverman, software designer”) who flooded Usenet cryptography groups with hostile postings in an attempt to start flame wars so caustic that they would homeopathically destroy the cypherpunks’ naive belief in the virtues of cryptography. That Detweiler meant this as a performance is further indicated by how rarely he took advantage of anon.penet.fi to secure a genuinely anonymous message. Although he often copied the signatures of others, Detweiler did not eliminate information in his header that revealed him as the author of these messages.

Whatever his initial motivations, Detweiler seems to have become en-
snared within his own increasingly vicious game. Most disturbingly, he began posting anti-Semitic messages apparently signed by Tim May on soc.jewish.culture. As Detweiler undoubtedly intended, May was promptly flooded with disgusted responses from members of soc.jewish.culture who were unaware that they were being manipulated. (As a result of this stunt, May said, Detweiler has been blocked from the Colorado State University network, but he has managed to obtain commercial Net access.) Although Detweiler’s crusade aims to expose the dangers of unsigned writing, the volume and hectoring force of his language show how involved he has become in his characters’ invented lives. Indeed, Detweiler—who sometimes posts thirty-five messages a day—must spend nearly all his waking hours browsing newsgroups or responding to opponents.

For all the damage inflicted by Detweiler, his behavior at least offers a lunatic lesson in Net operations. Other forms of networked secret writing are more directly malignant. During 1994, the Usenet’s Bosnia group (soc.culture.bosna.bergyna) was flooded with anti-Armenian messages from one “Serdar Argic,” advancing the thesis that the Turkish massacre of two million Armenians in 1915 was in fact a slaughter of Turks by Armenians. Argic is capable of flights of composition that dwarf even Detweiler’s: according to Usenet moderator Joel Furr, on one day in April 1994, 175 of the 210 messages on the group had been composed by him. Interviewed by Jon Weiner in the Nation, Furr indicated that “‘Serdar Argic’ seems to be several people, anti-Armenian Turks, with software that scans bulletin boards for keywords and automatically generates responses out of a database of megabytes of messages.”

I, Oedipa Maas

Although the Argic case is structurally the inverse of Detweiler’s (instead of a Medusan multiplication of speaking heads, Argic represents the work of several people, consolidated through a synthetic text generator), both illustrate how electronic writing relies on weak information about the identities of its virtual members. One reason for introducing myself as an actor in the preceding pages is to give some sense of the uncanniness of these identities, which, when they decay, generate pathologies familiar from postwar American politics and fiction. When we move into the Net, that is, we enter a space in which The Crying of Lot 49 reads as a documentary text, prefiguring the behavior of characters such as Detweiler and May. When Tim May writes that “I haven’t gotten any calls from Detweiler, to my knowledge, just some strange hang-ups in the middle of the night,” it is hard for me not to recall Oedipa Maas in The Crying of Lot 49, wakened at 3:00 A.M. by Pierce Inverarity, calling in the voice of Lamont Cranston. And Detweiler’s Medusa complex is worthy of Dr. Hilarius, Oedipa’s “shrink or psychotherapist,” in his most psychotropic moments. Net users often obliquely
refer to *The Crying of Lot 49*, identifying their workplace as “Yoyodyne Propulsion Systems,” with Yoyodyne serving as a generic title for military-industrial research. Pynchon even appears in May’s “infamous” signature as part of a dozen subversive topics:

<table>
<thead>
<tr>
<th>Timothy C. May</th>
<th>Crypto Anarchy: encryption, digital money</th>
</tr>
</thead>
<tbody>
<tr>
<td>W.A.S.T.E.: Aptos, CA</td>
<td>anonymous networks, digital pseudonyms, zero</td>
</tr>
<tr>
<td>Higher Power: 2756839</td>
<td>knowledge, reputations, information markets,</td>
</tr>
<tr>
<td></td>
<td>black markets, collapse of governments.</td>
</tr>
<tr>
<td></td>
<td>W.A. S.T.E.: Aptos, CA</td>
</tr>
<tr>
<td></td>
<td>Higher Power: 2756839</td>
</tr>
<tr>
<td></td>
<td>Public Key: PGP and MailSafe available.</td>
</tr>
</tbody>
</table>

Still, one may wonder: what does *The Crying of Lot 49* tell us about the Net that we would not have known otherwise? My answer is that the character of Oedipa lays out more clearly than any other in postwar fiction the contemporary stakes with regard to the cryptographic imagination. The issues raised by her experience—of the relation of identity to language, anonymity, and paranoia—echo the main themes of the Detweiler flame war. Like Oedipa, we as readers are divided between unsatisfactory reactions to telecommunications culture, forced to choose between an epistemological skepticism so great that it turns to paranoia (the Eliotic mode) and an unthinking spiritualization of technology. Pynchon’s novel beautifully plays out this division. Indeed, in a final turn of the cryptographic screw, I almost began to wonder if *I* had not written *The Crying of Lot 49*. The book’s nominal author was nowhere in evidence, and it uncannily presented all the motifs of this study, including Poe, spiritualism, telecommunications, information theory, World War II, the textual construction of Jacobean drama, and the question of who, exactly, wrote Shakespeare’s plays, all summoned under the aegis of cryptography.

Certainly, Pynchon’s Internet prominence follows partially from his interest in cryptography. Noting that *V* is preoccupied “with signs, codes, signals, patterns, plots, etc.,” Tony Tanner observes that “the preoccupation—not just the signals and patterns themselves—could be said to be the subject of the book.” He expressly describes Oedipa as “a cryptologist,” given over to “an unending effort to discover whether the will itself contains a code which she has to interpret; or whether in fact the will has been tampered with and a false code inserted in order to distract her from discovering the revelations of the will.” The “Mr. Thoth” in decline at Vesperhaven is named for the Egyptian god of wisdom, the inventor of letters and numbers, and therefore of writing; Pynchon also obliquely refers to the hieratica, a private hieroglyphic code used by the Egyptian priesthood. When Oedipa sees San Narciso for the first time, it looks to her like a printed digital circuit, and she finds that “there were to both outward patterns a hieroglyphic sense of concealed meaning, an intent to communicate.”

Ambiguously in league with this intent to communicate is the Tristero,
an international, violently anonymous, virtually immortal network designed to transmit secret writing. From certain angles, the Tristero (about which Oedipa learns from the “decrypted journals of the Comte Raoul Antoine de Vouziers, Marquis de Tour et Tassis”) resembles the NSA, which similarly forbade its employees from acknowledging the agency’s existence. Even more dramatically, though, the Tristero resembles the Internet in its intertwined transmission of the most reputable forms of writing (scientific research, professional notes, White House communiqués) alongside a subversive W.A.S.T.E.-like system, in which hundreds of subcultures pass secret missives. (What is the distance from the Inamorati Anonymous to alt.sexabuse.rec? How far is it from the fired Yoyodyne executive placing his classified ad to alt.suicide?) To be sure, most Net messages are as banal as the message received by Pynchon’s Mike Fallopian, written only to keep up the volume of transmissions: “Dear Mike. How are you? Just thought I’d drop you a note. How’s your book coming? Guess that’s all for now.” But the fantasy of communication that the Net produces is a potent element in its success and, like the postal system itself, it is one of the material institutions that determine the shape and range of our freedoms.

Published in 1966, The Crying of Lot 49 is contemporaneous with the cryptoliterary culture described in chapter 6 above, appearing one year after both The War of the Secret Agents and The Looking-Glass War. Yet in The Crying of Lot 49, cryptography is not primarily linked to Allied subterfuge. Whereas Le Carré’s cryptographic foci are an ancient radio transmitter and a silk inscribed with number groups, Pynchon’s are the Tristero and Inverarity’s will; whereas Le Carré’s novels are organized around the political divisions of the Cold War, Pynchon’s battle is fought within America, over such megacorporations as “the Galactronics Division of Yoyodyne, Inc.,” “a prolonged scatter of wide, pink buildings, surrounded by miles of fence topped with barbed wire and interrupted now and then by guard towers . . . two sixty-foot missiles on either side and the name YOYO DYN E lettered conservatively on each nose cone” (25).

But Pynchon’s novel and the Internet are both the result of World War II cryptography, and they can be read as parallel histories. In addition to the ruthless binarism of Cold War culture, with its absolute but reversible distinctions between patriot and traitor, American and Soviet, signifier and signified (the narrative material exploited by the school of Le Carré), the legacy of World War II cryptography includes the intellectual bequest of cybernetics, game theory, and the digital electronic computer (built “for the express and ultimately successful purpose of cracking the Germans’ key Enigma cipher”). Wartime research also led directly to Bell Labs engineer Claude Shannon’s “momentous postwar discovery of the foundations of information theory—a sophisticated mathematical abstraction of the dynamic between chaos (noise) and intelligibility (signal) in communica-
tions channels.”78 Shannon’s theory, set forth in “A Mathematical Model of Communication” (1948), finds its counterpart in his “Communication Theory of Secrecy Systems,” published in the Bell System Technical Journal the next year.79 As Shannon recalls, his work on information theory and cryptology were “so close together you couldn’t separate them.”80

As readers of Pynchon criticism know all too well, the references to information theory that permeate The Crying of Lot 49 (from the vision of San Narciso as a giant telecommunications circuit to Oedipa’s wayward can of hair spray, whizzing about on a statistical trajectory that “something fast enough, God or a digital machine, might have computed in advance”)81 have proved to be a critical dead end. Although Pynchon seems to set himself the task of aligning the different senses of entropy (one drawn from mechanics, the other from information theory) through the Nefastis machine, as several critics have noted, the entropy of mechanics means the inverse of the entropy of information theory. Pynchon’s attempt to pun his way across the two is a literary maneuver, not a scientific one: a master trope, but not a master narrative.82 What really animates Pynchon is not so much information theory as it is the more primary cryptographic imagination, which in The Crying of Lot 49 seeks to name the matrix in which matter and thought intersect.

In an odd way this resembles the question, so central to Pynchon’s novel, of whether one is identical with one’s words. For Emory Bortz, the answer is yes: his Shakespeare is simply the sum of those texts attributed to him. This is also true for Mucho, who discovers an LSD-fired ability to perform spectrum analysis in his head, breaking down “chords, and timbres, and words too into all the basic frequencies and harmonics, with all their different loudnesses,” and listening to them, “each pure tone, but all at once.” Such experience leads Mucho, a disc jockey, to conclude that “everybody who says the same words is the same person if the spectra are the same only they happen differently in time, you dig?”83 Mucho’s faith in the radio’s invisible waves reveals his kinship with Doten and her fellow spiritualists: each envisions technology as a way to make experience sacred once again.

As a would-be listener to the dead Inverarity, Oedipa experiences the world as a form of posthumous speech, and, like Lizzie Doten, her problems begin with intrusive voices—in her case, the sleep-shattering ring of Inverarity’s telephone call. From that moment on, the novel interrogates forms of information transmission, including speech, sex, letter writing, telephones, television, cinema, radio, and telepathic manipulation. Voices blend: after Inverarity’s death, Oedipa is again awakened, this time by Hilarius, sounding “like Pierce doing a Gestapo officer,” who was moved to call by “this feeling. Not telepathy. But rapport with a patient is a curious thing sometimes.”84 Oedipa is seduced by Metzger in front of the television, and forced to endure both the music of the Paranoids, the heavily amplified band run by
Miles, and that performed in the Yoyodyne bar, where the means of amplification have become the instruments ("we got a whole back room full of your audio oscillators, gunshot machines, contact mikes, everything man").

The Crying of Lot 49 is written in Poe's wake. References to Poe appear in The Courier's Tragedy, whose third act alludes to "The Masque of the Red Death" and to the central drama of Poe's bitter little story "Hop-Frog," in which a hunchbacked court jester exacts revenge on the king and his court by persuading them to dress up for a costume ball as a set of apes chained together. But the most salient allusion to Poe occurs when, having mailed the letter for the old sailor, Oedipa waits by the trash can, determined to know if the W.A.S.T.E. system really exists. "Towards midday a rangy young wino showed up with a sack; unlocked a panel at the side of the box and took out all the letters." Oedipa follows him by foot and by bus, from San Francisco to Oakland and from Oakland to Berkeley, where "halfway up Telegraph the carrier got off and led her down the street to a pseudo-Mexican apartment house. Not once had he looked behind him. John Nefastis lived here. She was back where she'd started, and could not believe 24 hours had passed." As in Poe's story, Oedipa's wandering eventually returns her to the place from which she had started, but midway through her San Francisco Walpurgisnacht, Pynchon's woman of the crowd has her attention fixed by the hidden systems of American community.

By repeatedly echoing "The Man of the Crowd," Pynchon signals a relation between his work and that of Poe. In Poe's tale, the unnamed narrator—a failed flâneur captivated by an inscrutable old man walking in the streets—makes the mistake of allowing his curiosity to lead him from the confines of his café into the unreflective and debilitating motion of the crowd. In search of amusement, he comes away "wearied unto death" (PT, 396) by the ceaseless motion embodied in the old man's erring. Oedipa, too, is fascinated by the social life of the city, but for her the mystery lies in the mechanisms by which ordinary people escape the sameness of their lives, converting waste into W.A.S.T.E., an empire of invisible writing in which they invest their hidden selves. This is cryptography in its most social sense, Pynchon's transvaluating imagination of the will to conspiracy that has driven American culture since the days of Andrew Jackson and George Lippard. In "The Man of the Crowd," the physiognomic logic that drives Poe's detective fiction breaks down: the narrator's efforts with the old man (a figure for the mystery of urban experience) collapse. But whereas Poe's narrator recoils from his object, Oedipa becomes implicated in the Tristero's recuperation of the wasted lives she comes to see everywhere, most particularly in the life of the old sailor.

Oedipa's imagination of the sailor's death centers on "the massive destruction of information" that will accompany his passing: "So when this mattress flared up around the sailor, in his Viking's funeral: the stored,
coded years of uselessness, early death, self-harrowing, the sure decay of hope, the set of all men who had slept on it, whatever their lives had been, would truly cease to be, forever, when the mattress burned. She stared at it in wonder. It was as if she had just discovered the irreversible process.”  

_Crying of Lot 49_ frames the bum’s death in terms of ciphers because everything within it, from the Bay Bridge to Oedipa’s innermost thoughts, is composed of hidden signs and figures. On the one hand, there are the messages of physics and engineering—the way in which Mucho’s crystalline audition of the pop song threatens to recreate the musician and his history whole in Mucho’s mind. On the other, there are the indices of Inverarity’s ambiguous texts, his mutilated stamps, his emended Jacobean dramas, and his middle-of-the-night calls. The book’s pathos is generated by Oedipa’s desire to make these messages coexist, to have the signs and symbols of the world speak in human terms. Cryptography is not only the source of information theory, which renders everything as interchangeable data; it is potentially a model for spiritual meaning too, as it pushes its practitioners to the limit where they confront the insoluble relations of mind and matter.  

A faith in disembodied mental power is part and parcel of the cryptographic imagination, whether it takes the form of Dupin’s power over the nail or of Doten’s channeling. Even William Friedman had a longstanding interest in ESP. In 1958 he wrote to William Baker, head of research at Bell Laboratories: “Now why didn’t the Bell people succumb to my needling them over the years that ESP is a form of communication. Bell Telephone goes in for studying communications: why not ESP?” Current investigations, he added, “may bring about a revolution of thought greater than that brought about by Copernicus.” Unlike Doten, both Oedipa and Friedman fail in their attempts to unify matter and spirit. (This is true, too, of Oedipa’s spiritualist precursor: in 1854, a “Mrs. ————” under the tutelage of the Universalist minister John M. Spear attempted to use her newly developed “Motive Power” to run a motor that Spear had designed. The machine refused to operate.) Although Pynchon frames this unsuccessful hierophancy in the esoteric vocabulary of information theory (how does one tell a message from noise?), _Crying of Lot 49_ suggests that we are all cryptographers forced to puzzle over the text of the world. Our resources are limited: only the “compiled memories of clues, announcements, intimations, but never the central truth itself, which must somehow each time be too bright for her memory to hold” (95), the “gemlike clues” that are only “some kind of compensation. To make up for her having lost the direct, epileptic Word, the cry that might abolish the night” (ibid., 118).  

Although the texts puzzled out here vary, they all seem to turn on words from the dead. In the penultimate scenes of _Crying of Lot 49_, Oedipa’s attention returns to the question of Inverarity’s will, in both senses of the word. Pynchon’s testamentary language is that of encryption and enigmas:
Might Oedipa Maas yet be his heiress; had that been in the will, in code, perhaps without Pierce really knowing, having been by then too seized by some headlong expansion of himself, some visit, some lucid instruction? Though she could never again call back any image of the dead man to dress up, pose, talk to and make answer, neither would she lose a new compassion for the cul-de-sac he’d tried to find a way out of, for the enigma his efforts had created. . . . He might have discovered The Tristero, and encrypted that in the will, buying into just enough to be sure she’d find it. Or he might even have tried to survive death, as a paranoia; as a pure conspiracy against someone he loved. . . . Had something slipped through and Inverarity by that much beaten death? (Ibid., 178–79)

This book is an investigation into the will as an ur-text for literature, as a model for the way texts covertly seek to write themselves into those who inherit them. Pynchon’s novel perfectly captures the sense of being obscurely imposed on by such fictions. This sense of imposition returns us to the way in which Poe’s writing has been felt by so many of his readers as a kind of pressure, ranging from the transformative gale of language felt by Lizzie Doten to the sinus-cold congestion of T. S. Eliot, and including in between such odd bedfellows as Charles Baudelaire, Rufus Griswold, Jorge Luis Borges, John Henry Ingram, Princess Marie Bonaparte, William Friedman, and Jacques Lacan.

Fame, writes Borges, is a form of incomprehension. The band of Poe’s followers assembled in these pages provides memorable evidence for Borges’s position, for they are united only in their fascination with the permanence and revelatory force of writing. However diverse their redactions of Poe, these figures agree that the preservation of human experience through writing is—literally—an inhuman desire, an attempt to replace mortality with immortality. This impulse behind cryptography is as old as Christ’s transfiguration, a harrowing in which Logos emerges radiant and eternal. Reading Poe through his followers’ eyes, we see that in the twentieth century, literature got what it always sought. Poe represents the realization that the telos of literature was always telecommunications, an ultimate, immanent script.

Earlier, Oedipa observed the aerial resemblance of San Narciso to a printed digital circuit, finding in both “a hieroglyphic sense of concealed meaning, an intent to communicate.” The Crying of Lot 49 refuses to make the choice between “transcendent meaning” or “only the earth” (ibid., 181). But if Pynchon’s novel ends before the unveiling of the Tristero, Pynchon also indicates that in our search for revelation in an age of telecommunications, we remain at the mercy of the written word. Reprimanding Oedipa for her “Puritan” obsession with the text of The Courier’s Tragedy, Randolph Driblette insists: “It isn’t literature, it doesn’t mean anything. Wharfinger
was no Shakespeare.' ‘Who was he?’ she said. ‘Who was Shakespeare? It was a long time ago’" (ibid., 77). When Oedipa asks for information about “the historical Wharfinger,” Emory Bortz makes a similar observation:

“The historical Shakespeare,” growled one of the grad students through a full beer, uncapping another bottle. “The historical Marx. The historical Jesus.”

“He’s right,” shrugged Bortz, “they’re dead. What’s left?”

“Words.”

“Pick some words,” said Bortz. “Them, we can talk about.” (Ibid., 151)

_The Crying of Lot 49_ is nothing but words: words about our attempts to establish legacy, relation, ownership, and, above all, identity, in ways that can never be more secure than the shifting lines of script themselves.

In this respect, Pynchon remains committed in an old-fashioned way to the powers and limits of language. Hence, the conclusion to _The Crying of Lot 49_ inverts that given by Gibson in _Neuromancer_, which, despite its urban sprawl and moral degeneration, turns out to be sentimental about, of all things, the hieroglyph. By concluding with the vision of Case doubled in the computer, _Neuromancer_ commits itself to a faith that language (or data) might still offer a type of immortality. By contrast, the force of Pynchon’s novel is to deny this sort of hieroglyphic prosopopoeia. No matter how well Inverarity has coded himself into his writing, his original identity dies. His only chance of survival is like Poe’s with Lizzie Doten or Baudelaire, as a “pure conspiracy against someone he loved”—as, that is, a will couched in the form of script.

Such script may be electronic. The millions of Internet users are all cousins of Oedipa Maas. Like her (or like me, in my search for Detweiler), they may be altered by their exchanges, perhaps even wrenched into new sorts of lives, although they may never be sure of the identity of their electronic correspondents. The Internet is like Inverarity’s will written on an even grander scale. Like Pierce’s businesses, the source of the wealth that gave his will muscle, the Internet is an unholy child of the military and the government, created for purposes that seem malevolent but that are capable of being twisted otherwise. If the Net offers new promises to a post–Cold War culture, it is not because on it a disembodied free speech and opportunity prevail, but because in its distortions we can witness our own alienated fears and desires, in a “secular miracle of communication” that we can only write for ourselves.\(^95\)