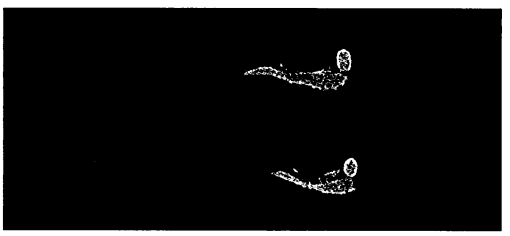
sis imperfecta. The mutant initially caught her attention with its small size. When she x-rayed it, she found a mass of broken ribs. On closer inspection of the mutant strain, she found that it forms cartilage normally during early development, but its bones in adulthood are fragile. Although she has not identified the exact mutation at fault, it seems to be near a collagen-encoding gene fingered in human cases of osteogenesis imperfecta. Fisher suspects that this mutant strain could prove valuable for research into collagen's role in bone formation and maintenance.

Whereas broken bones are relatively easy to spot, problems in biochemistry can be harder to detect, even in the see-through zebrafish. But here, too, scientists are hoping the animal will help answer some difficult questions. Steven Farber of Thomas Jefferson University in Philadelphia and Michael Pack of the University of Pennsylvania School of Medicine in Philadelphia and their colleagues have devised a way to observe the biochemical reactions of digestion in living zebrafish. To identify genes that regulate one part of digestion, lipid processing—known to influence the development of colon cancer, heart disease, and other human ills—the team has designed lipid molecules that glow when they are digested by a key enzyme in the intestine. When the scientists feed this molecule to zebrafish larvae, they can see the molecule light up in the digestive tract and liver and then travel to the gallbladder. Although the screen is in its early stages and the scientists have only begun to identify potential mutants, developmental biologist Didier Stainier of the University of California, San Francisco, is impressed. "If you can actually ask questions about how these intestinal cells are processing a substrate, that's very powerful," he says. The team hopes to design other molecules to probe the digestion of carbohydrates and other molecules. "We're visualizing biochemical processes in living vertebrates," says Farber. "Zebrafish is the only game in town where you can do that."



Healthy glow. A custom-made lipid, designed to identify fish with faulty digestion, lights up in the digestive tract of zebrafish larvae.

The most difficult part of the process is still tracking down the mutant gene itself, but scientists say that ongoing work in zebrafish genomics is making that task easier. And the likely launch of an effort to sequence the zebrafish genome (*Science*, 5 May, p. 787) will also ease that task. Genome projects in the mouse and human, says developmental biologist Nancy Hopkins of the Massachusetts Institute of Technology, will only make the zebrafish more important. Those projects will turn up thousands of unknown genes, she says, and it is likely to be easier to figure out what they do in the fish. Says Hopkins: "We've barely begun to tap" the potential of zebrafish. **–GRETCHEN VOGEL**

DIGITAL ENCRYPTION

Algorithmic Gladiators Vie For Digital Glory

As NIST zeroes in on a new cryptographic standard, the competitors scramble to face an unforeseen threat—from lawyers

And then there were five. For 2 years, glory-seeking cryptographers from across the globe have been cracking one another's ciphers, trying to establish their own algorithms as the new standard in encryption. In mid-April the five finalist teams faced off in New York. They subjected each other's algorithms to the withering fire of cryptographic attack after cryptographic attack, while judges observed the melee. But as the smoke cleared, the contestants found themselves facing a menace from a new and unexpected quarter: the realm of patent law.

The five finalist algorithms—MARS, Twofish, Rijndael, RC6, and Serpent—are vying to be the new standard in encryption, replacing the aging Digital Encryption Standard (DES), endorsed by the National Bureau of Standards in the mid-'70s. Thanks to the government's stamp of approval, DES has become perhaps the most widely used encryption system in the world. The new algorithm, selected by the National Institute of Standards and Technology (NIST)—the Bureau of Standards' successor—will replace DES and should assume its mantle of preeminence. No money is at stake in the competition; under NIST's licensing terms, the inventor of Advanced Encryption Standard (AES) will not benefit financially. "The big thing, personally, is the fun of doing it," says John Kelsey of Counterpane Internet Security in San Jose, California. "If you're in block ciphers, it's the coolest thing you can do, as far as I can tell."

Outside the arena, however, the stakes are serious indeed. If someone were to crack the AES a few years down the line, all the reams of data encrypted with NIST's standard could be compromised. Medical records, bank transactions, and other confidential information would potentially be wide open to anyone with the know-how, and it would take years for engineers to replace the cracked algorithm in smart cards, computers, and descrambler boxes.

Fears of such a breach are what drove officials to seek a replacement for DES in the first place. DES was designed to take a stream of digital data, split it into 64-bit chunks, and encipher it. In theory, an eavesdropper could not decipher the data without guessing the 56-bit cryptographic "key" that opens the cipher—a secret shared by only the sender and intended receiver.

By the early 1990s, fissures had begun to show in DES's security. Cryptographers such as Eli Biham and Adi Shamir of the Technion–Israel Institute of Technology in Haifa developed new attacks such as "differential" cryptanalysis, in which a cryptographer tries to crack an algorithm by feeding very slightly different data into it and comparing how the encrypted outputs differ. As a result, instead of having to guess 56 bits of a key (which requires a search through 2^{56} possible keys), would-be crackers could decipher the message after trying only 2^{46} keys or so—a 1000-fold improvement. More important, computers got faster. DES was being cracked by brute-force searches in which speedy computers simply tried every possible key. Last year, in response to a challenge by the San Jose–based cryptography company RSA Security, volunteers yoked nearly 100,000 PCs together via the Internet to decipher a DES-encrypted message. They succeeded in less than a day. To beef up security, wary DES users started running the algorithm three times with three different keys. NIST, however, decided that patches were not enough. In 1997, the institute called for a new standard; the AES contest was born.

Cryptographers from all over the world submitted candidate algorithms, from which NIST selected 15. Two years and a lot of code-cracking and skirmishing later, NIST narrowed the field to five finalists—and the international cryptographic community turned its attention to testing, and breaking, them.

On 13 and 14 April, participants in the

CREDIT: W. LIEDTKE AND J. FRIEDMAN/HHMI AND THE ROCKEFELLER UNIVERSITY

cryptanalytic demolition derby gathered in New York to present their results at the third AES conference, the final gathering before NIST chooses a standard late in the summer. "It's the last AES conference. I'm thankful," sighed NIST's Jim Foti. An overhead projector aimed at a screen at the front of the room greeted participants with an apt image: King Kong perched atop the Empire State Building, under attack by a swarm of biplanes.

As cryptographic algorithms go, the five rival contestants are 500-pound gorillas themselves. Each employs a key 128, 192, or 256 bits long—potentially much more secure than the 56-bit key of DES. In broad terms, they all do the same thing, taking a 128-bit chunk of text and jumbling it up and changing the bits so that they become unreadable. Each scrambling algorithm is publicly available; even if an eavesdropper knows exactly how the encrypting machine works, the knowledge is useless without the key.

An important feature of a secure cipher is that a tiny change in the cryptographic key makes a huge difference in the scrambled output. As a result, guessing part of a key doesn't give any information about the text or about the rest of the key. Ideally, even if an eavesdropper guesses 127 of the 128 bits in the key, the message decrypted with this "key" should be just as unreadable as if he used a random key. This small-key-changes-yield-huge-output-changes feature is called "nonlinearity."

Four of the five algorithms create nonlinearity the way DES does, through devices called "S-boxes." An S-box takes a string of ones and zeros and returns a different set; it's essentially a look-up table that converts one string to an unrelated one, turning small changes in input into large changes in output. IBM's entry, MARS, boasts an S-box–based cryptographic "core" surrounded by a "wrapper" of lighter weight scrambling subroutines that protect the core from direct cryptanalytic assault. Serpent, designed by Biham and partners in Britain and Norway, passes information through eight S-boxes over and over, cycling the text through many more "rounds" of manipulation than its competitors do before it spits out the encrypted data. Twofish, designed by Bruce Schneier of Counterpane and colleagues, changes the contents of the S-boxes depending on the cryptographic key, unlike the others, which have fixed S-boxes. Rijndael, the entry of two Belgian cryptographers, relies upon elegant mathematical manipulations of the data, arranged into a square; a single S-box adds nonlinearity.

The S-box–free algorithm is RC6, designed by RSA Security's Ron Rivest and other cryptographers in the United States and Britain. It takes slices of data and "rotates" them by cutting a chunk off one end and pasting it back on the other. The amount of rotation depends upon the data being rotated. Changing a single bit in a chunk of data tends to cause a change in rotation, altering the data quite a bit and changing how the data get rotated even more; small differences in data propagate and proliferate as the process repeats over and over, ensuring nonlinearity.

Code wars. Companies are vying to turn data into gibberish, but is the gibberish secure?

Choosing a winner among the finalists is no easy task. Even figuring out which algorithm runs fastest is almost an intractable problem, because of the huge number of different types of software and hardware the algorithm will run on. Rijndael appears to be the fastest overall, but most designers had to be content with a mixed showing, slow on some platforms and fast on others. Serpent, for example, is the quickest on field-programmable gate arrays—reconfigurable hardware devices—but the slowest on a Pentium. "Looking at all the performance requirements, we generally don't suck," says Twofish designer Schneier.

More important than speed is security. None of the algorithms has been broken, but some have been bloodied. Rijndael performs its mixing and jumbling operation 14 times before spitting out an answer. Cryptographers have figured out mathematical tricks to crack an eight-rounded variant with a lot less effort than guessing all the possible keys. Nine of 16 rounds in MARS have been cracked, as have 15 of 20 in RC6. The attacks are still theoretical—no computer today could use them to crack a cipher in any reasonable amount of time—but they might be cause for worry in the future. "Attacks are improved all the time," Biham says. "If an algorithm has a very small security margin, it will be attacked." Biham's entry, Serpent, edges out Twofish for the distinction of most secure algorithm, although the difference is probably academic. "It's a bank vault versus a bank vault with a bit of kryptonite in case Superman walks by," jokes Nicholas Weaver, a cryptographer at the University of California, Berkeley.

Some conference participants, meanwhile, worried about a different type of assault: patent attacks. Intellectual property was not an issue when cryptography was mostly a government-only preserve, but now that commercial companies are in the cryptography game, the playing field has changed. Days before the conference opened, the software division of Hitachi Ltd. wrote to NIST claiming that it holds a U.S. patent on techniques used in four of the finalist algorithms. Whether or not the claim holds up, NIST is entering a "quagmire" of potential intellectual property disputes, says Josh Benaloh of Microsoft Research. The more popular and widely distributed a NIST-sponsored standard becomes, the messier and more expensive the legal battles might be. "I think it's far more likely than the cryptographic attack," Benaloh says—and potentially much harder for cryptographers to handle.

"We are not lawyers up here, you know," Schneier says. "I'm at a complete loss at how to deal with various patent laws." Others share his bewilderment. "This is a very real attack. This is a very significant attack," says James Hughes of StorageTek in Minneapolis. Even a hint of patent trouble should disqualify a contender, Hughes says: "If it happens, I suggest that NIST withdraw its suggestion immediately and pick another." For NIST, the possibility of patent troubles just serves to make a tough call even tougher. Any choice it makes will satisfy some parties and anger others. Shamir alone claims to have found an easy solution. "No one algorithm is head and shoulders above the rest," he says. "I suggest having a fair coin flip."

—CHARLES SEIFE

ILLUSTRATION: TERRY SMITH