turian, substance P will be considered for inclusion in NIA's Alzheimer's drug development program, although he suggests that the neurotransmitter itself may not be a suitable drug. Substance P is a mediator of inflammation, as well as a neurotransmitter in the body's pain pathways, although Yankner says that the rats injected with it didn't show any signs of discomfort. The next step, everyone agrees, will be to see whether Yankner and Kowall's model can be duplicated in nonhuman primates, so that substance P's action can be tested in animals whose brains more closely resemble those of humans.

Whether those results can be duplicated in monkeys or not, Khachaturian says this latest development is "going to get everyone excited." Which isn't a trivial thing, because, he says, "science always does well when there's excitement." Next to be seen: whether that excitement will produce answers to the remaining puzzles in the Alzheimer's mystery. ■ JEAN MARX

Quantum Cryptography's Only Certainty: Secrecy

From the battles of the ancient Spartans to the cold war, people relaying secret messages have played a game of cat and mouse with code-cracking opponents. As message-senders employed more advanced encrypting techniques, enemies with increasingly sophisticated spying methods followed fast on their heels. But now physicists say the secretive mice may eventually rest safely, protected by the laws of quantum mechanics. Indeed, there's a friendly transatlantic competition afoot between physicist Charles Bennett of IBM's Thomas J. Watson Research Center and Oxford physicist Artur Ekert to see who can cloak messages in the darkest quantum secrecy.

The uncertainty principle, which hides nature's finest details in perpetual privacy, can protect a message from eavesdroppers, says Ekert. In the minute world of the atom, the uncertainty principle decrees that for certain pairs of properties—the position and momentum of a particle such as an electron or a photon, for example—the process of measuring one changes the other, making the combination of properties forever unknowable. "The laws of physics itself prevent you from knowing anything without disturbing the system," says Ekert. If a message could be encoded in such a pair of quantum properties, even the cleverest spy would leave an obvious fingerprint if he tried to read the message.

Physicists discussed the possibility of harnessing nature's secret-keeping ability as early as 1970, and Bennett devised the first quantum-mechanical scheme to relay messages in 1982. Now, in a paper in the 5 August *Physical Review Letters*, Ekert has presented his own brand of quantum cryptography.

All quantum cryptography schemes aim to protect the "key"—the secret string of numbers sender and receiver use to encode and decode messages. In modern cryptography, only the key needs to be kept confidential; the scrambled message can travel over an insecure channel such as the phone system.

In Bennett's original scheme, Alice and Bob (the two proverbial secret exchangers in cryptography), transmit a series of 0s and 1s—the binary code for the key—written in the polarization of individual photons. Polarization describes the vibrational direction of the electric field associated with the light. Alice sends each bit coded either in a photon's circular (rotating) polarization (left=1, right=0) or its linear polarization (horizontal=1, vertical=0).

Quantum link. *A secret, secure code emerges from the spins of correlated particles.*

These two types of polarization make up a pair of properties protected from measurement by the uncertainty principle. Measure one and the value of the other will be forever unknowable. An eavesdropper (traditionally named Eve) won't know which form of polarization to measure when she intercepts a passing photon. What's more, whichever form she detects, she'll end up affecting the other, leaving an impression on the photon's polarization that Alice and Bob will ultimately be able to detect. They could then discard the potentially compromised code.

To be sure of catching Eve in Bennett's scheme, Alice and Bob must compare notes for a series of individual photons. Ekert's competing scheme offers a shortcut: Under his plan, Eve would leave her fingerprint in the overall statistical properties of the system.

In Ekert's scheme, neither Bob nor Alice develops and sends the key. Instead, the information is created by the vagaries of quantum mechanics as pairs of subatomic particles are shot out in opposite directions by the decay of a single atom. The particles carry a quantum-mechanical property called spin, which is measured as either "up" or "down." Bob and Alice, waiting to receive particles from the central source, are both equipped with detectors that measure spin along a given axis. They vary the orientation of their detectors at random as they make their observations.

According to the laws of quantum mechanics, the spins of the two particles emitted by each decay are correlated. In the simplest case, if both Bob and Alice are holding their spin detectors in the same orientation and one detects an "up" particle, the other must be detecting a "down" particle. But those correlations would be disturbed if an eavesdropper made a measurement along some other axis.

Thus the correlations give Bob and Alice the common information they need to create—and protect—their key. Bob and Alice have to confer afterward to figure out when their detectors were in the same orientation, but once they share that information, each knows what the other must have measured. If Bob measured up, Alice must have measured down—or vice versa. By prior arrangement, one outcome represents a 1, the other a 0 in the key. Since the spin measurements should show an overall statistical correlation even when the detectors were oriented differently, Bob and Alice can foil Eve just by examining the statistics of the measurements they aren't including in the key. By the uncertainty principle, any eavesdropping will disrupt the correlations in these noncoding bits.

A variation of Ekert's strategy using photons has actually been tested in a room-sized experiment involving ultrafast detectors. Bennett's idea has also taken shape in a prototype device he and John Smolin developed in 1990 at IBM. But until the technology advances—and Ekert is confident it will—sending messages more than several meters will be out of reach of either scheme. At that distance, Bennett admits, it would be equally secure—and much easier—just to hand someone the message on a piece of paper. ■ FAYE FLAM