A rough road to the planets

The first to embark will be Magellan, setting out on April 27, 1989, to begin mapping Venus 16 months later. Galileo will depart less than six months after Magellan, bound on a six-year journey to Jupiter and its giant moons, visiting a pair of asteroids along the way. In October of 1990, Ulysses will venture forth to spend four-and-a-half years on a trek laid out to cross over both poles of the sun. Spectacular goals for a country that has not dispatched an explorer to another world in a decade.

At least that's the plan.

NASA periodically reaffirms that its goal in returning the space shuttle to flight is to do the job right, rather than "speed at any cost." Even so, the delay caused by the unexpected failure of a component during a test-firing of one of the craft's booster rockets last month (SN: 1/2/88, p.7) has focused attention on the long list of "payloads" waiting for a ride. And among the hardest pressed are the interplanetary missions, which can depart only when their destinations are in their proper orbital positions, and which therefore risk huge delays if they miss their "launch windows."

Having abandoned hope of getting the shuttle off the ground by June 2, the space agency this week tentatively announced a revised and approximate date. "The earliest possible would be mid-July," said shuttle chief Richard Truly, "but it's more likely to be in the August time frame."

At the same time, he announced that the design of the part that failed, an "outer boot ring" intended to protect the rocket nozzle from hot exhaust gases, has been replaced with a version used in a successful test-firing last summer. Still, additional testing remains.

NASA has long been aware that its timetable for bringing the shuttle back allows little margin for unexpected sources of delay, but now the itinerary is even tighter. There are four shuttle flights ahead of Magellan, for example, and even a slight postponement could set back the spacecraft's launching by more than two years, says project manager John Gerpheide of Jet Propulsion Laboratory in Pasadena, Calif. There's a possible launch window only six months after the planned one, but it occurs right around the planned Oct. 8 launch of the Galileo, and NASA is extremely reluctant to risk the strain on launch personnel and available checkout time of sending off two major planetary missions in the same month. Another chance for Magellan would come along 13 months after that, but attention then will be directed at launching the European Ulysses spacecraft, which must fly out to and around Jupiter to set up the inbound path over the sun's poles. With both possibilities essentially unavailable, says Gerpheide, Magellan must either take off next year on schedule or wait until May 25, 1991.

Galileo, meanwhile, is locked to its own calendar for an even more intricate set of reasons. Jupiter reaches a desirable position in its orbit for flights from earth about every 13 months, but safety concerns following the Challenger disaster prompted NASA to cancel the liquid-hydrogen-burning Centaur upper-stage rocket that the shuttle would have carried up to send Galileo on its way. As a result, Galileo will be using a less energetic upper-stage, which must direct the spacecraft onto an incredibly complicated trajectory that will take it through a gravitational "swing-by" of Venus followed by two of earth. Even with no other launchings in the way, a Galileo delay would slip it, too, to mid-1991.

Due for launch on June 1, 1989, is the long-awaited Hubble Space Telescope (SN: 6/23/84, p.392), which many astronomers feel may virtually revolutionize their field. To be stationed in earth-orbit, it will not need to wait for launch until other planets have lined themselves up. But sustaining the large scientific and engineering teams dedicated to this project, as well as those needed for Magellan and Galileo, is costing NASA more than $100 million a month. *– J. Eberhart*

Computing a bit of security

It sounds like a children's game: proving that you know a particular password without having to give away any hint of what the actual password is. Yet such a scheme is at the heart of several recently proposed methods for keeping information – whether in the form of an access code, identification number or message – secret during transactions involving computers. Successfully implemented, these methods would make computer operations such as transferring funds, signing contracts and sending and receiving sensitive information more secure. Neither eavesdropper nor receiver would be able to hijack enough information to masquerade as the sender.

The methods involve a mathematical concept that goes by the name of "zero-knowledge" or "minimum-disclosure" proof. Most schemes involving zero-knowledge proofs are interactive (SN: 8/30/86, p.140). The idea is to set up a dialogue between the "prover" (for example, a bank-card bearer who would like to prove that he can legitimately withdraw a certain sum of money) and the "verifier" (say, a bank). The verification process works if the prover's identity is tied to a mathematical statement for which the prover but not the verifier or a potential eavesdropper has a proof.

One such identification method, proposed by Uriel Feige, Amos Fiat and Adi Shamir of the Weizmann Institute of Science in Rehovot, Israel, depends on the observation that while it's relatively easy to determine whether a number is prime (divisible only by itself and 1), finding the factors of a large composite number is difficult and time-consuming (SN: 3/30/85, p.202). By following the mathematical procedure built into the Shamir scheme, the prover uses his knowledge of the prime factors of a large number to persuade a verifier, who knows the number but can't factor it, that his "signature" is valid.

"The result is striking," comments computer scientist Susan Landau of Wesleyan University in Middletown, Conn., in this month's NOTICES OF THE AMERICAN MATHEMATICAL SOCIETY. "Smart" identification cards containing a computer chip could be programmed to conduct the protocol, she says. However, without further safeguards, card theft would be a problem.

The Shamir method, like many other digital signature and identification schemes, may also fail if a third party, unknown to the prover and verifier, surreptitiously acts as a go-between, transferring information between the prover and verifier. "It's the problem of active eavesdropping," says Fiat, who is presently at the University of California at Berkeley. The eavesdropper may be not only listening in but also making changes in the conversation.

In attempts to overcome such problems and to speed up verification, researchers have been exploring variations of the basic zero-knowledge method. At last week's meeting in Atlanta of the American Mathematical Society, one group proposed a protocol that allows the prover to give away some information for the sake of efficiency. In this scheme, as described by Claude Crépeau of the Massachusetts Institute of Technology, information is represented as blocks, each with a value of 0 or 1. The prover, depending on the verifier's request, can reveal either the value of a block or that two blocks have the same value (without giving away the value). This idea can be converted quite readily into a practical mathematical procedure and computer protocol.

In another variation, Manuel Blum of the University of California at Berkeley and MIT's Silvio Micali recently found a way to make zero-knowledge proofs noninteractive. With their method, the prover can publish the fact that a theorem is true without revealing the proof and without the active participation of a verifier. *– I. Peterson*