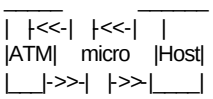
Dial: 267-0293
Sent: ********2670293
* - Denotes the originating number which is coded and sent before the number

As you noticed there are 8 digits in the coded number. This is because, at least I believe, it is stored in a binary-like form. Automatic Number Identification means a limited future in phreaking. ANI does not threaten phreaking very much yet, but it will in the near future. A new switching system will soon be installed in most cities that are covered by ESS, Electronic Switching System, now. The system will have ANI capabilities which will be supplied to the owners of phone lines as an added extra. The owner's phone will have an LED read-out that will show the phone number of the people that call you. You will be able to block some numbers, so that people cannot call you. This system is in the testing stages currently, but will soon be installed across most of the country. As you see, this will end a large part of phreaking, until we, the phreakers, can come up with an alternative. As I have been told by several, usually reliable, people, this system is called ISS, which I am not sure of the meaning of this, and is being tested currently in Rhode Island. 800 in-watts lines set up by AT&T support ANI. The equipment to decode an ANI coded origination number does not costs as much as you would expect. 950 ports do not offer ANI capability, no matter what you have been told. The 950 ports will only give the city in which they are based, this usually being the largest in the state, sometimes the capitol. One last thing that I should tell you is that ANI is not related to tracing. Tracing can be done on any number whether local, 950, etc. One way around this, especially when dialing Alliance TeleConferencing, is to dial through several extenders or ports. ANI will only cover the number that is calling it, and if you call through a number that does not support ANI, then your number will never be known.

68. Jackpotting ATM Machines by The Jolly Roger

JACKPOTTING was done rather successfully a while back in (you guessed it) New York. What the culprits did was sever (actually cross over) the line between the ATM and the host. Insert a microcomputer between the ATM and the host. Insert a fraudulent card into the ATM. (By card I mean cash card, not hardware.) What the ATM did was: send a signal to the host, saying "Hey! Can I give this guy money, or is he broke, or is his card invalid?" What the microcomputer did was: intercept the signal from the host, discard it, send "there's no one using the ATM" signal. What the host did was: get the "no one using" signal, send back "okay, then for God's sake don't spit out any money!" signal to ATM. What the microcomputer did was intercept the signal (again), throw it away (again), send "Wow! That guy is like TOO rich! Give him as much money as he wants. In fact, he's so loaded, give him ALL the cash we have! He is really a valued customer." signal. What the ATM did: what else? Obediently dispense cash till the cows came home (or very nearly so). What the crooks got was well in excess of $120,000 (for one weekend's work), and several years when they were caught. This story was used at a CRYPTOGRAPHY conference I attended a while ago to demonstrate the need for better information security. The lines between ATM's & their hosts are usually 'weak' in the sense that the information transmitted on them is generally not encrypted in any way. One of the ways that JACKPOTTING can be defeated is to encrypt the information passing between the ATM and the host. As long as the key cannot be determined from the ciphertext, the transmission (and hence the transaction) is secure. A more believable, technically accurate story might concern a person who uses a computer between the ATM and the host to determine the key before actually fooling the host. As everyone knows, people find cryptanalysis a very exciting and engrossing subject..don't they? (Hee-Hee)



The B of A ATM's are connected through dedicated lines to a host computer as the Bishop said. However, for maintenance purposes, there is at least one separate dial-up line also going to that same host computer. This guy basically BS'ed his way over the phone till he found someone stupid enough to give him the number. After finding that, he had has Apple hack at the code. Simple.

Next, he had a friend go to an ATM with any B of A ATM card. He stayed at home with the Apple connected to the host. When his friend inserted the card, the host displayed it. The guy with the Apple modified the status & number of the card directly in the host's memory. He turned the card into a security card, used for testing purposes. At that point, the ATM did whatever it's operator told it to do.

The next day, he went into the bank with the $2000 he received, talked to the manager and told him every detail of what he'd done. The manager gave him his business card and told him that he had a job waiting for him when he got out of school.

Now, B of A has been warned, they might have changed the system. On the other hand, it'd be awful expensive to do that over the whole country when only a handful of people have the resources and even less have the intelligence to duplicate the feat. Who knows?

69. Jug Bomb by The Jolly Roger

Take a glass jug, and put 3 to 4 drops of gasoline into it. Then put the cap on, and swish the gas around so the inner surface of the jug is coated. Then add a few drops of potassium permanganate solution into it and cap it. To blow it up, either throw it at something, or roll it at something.

70. Fun at K-Mart by The Jolly Roger