A

report

on

“ATM”

Submitted in partial fulfillment of the requirement for the JAVA Internship

SUBMITTED TO:
PW Skills

SUBMITTED BY:
ABHISHEK SHARMA

Acknowledgement

I would like to thank respected **Mr Priya Batia** for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went throughmy work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work moreorganized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Preface

I have made this report file on the topic **ATM;** I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have triedto give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to **Priya Bhatia** who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidenceand most importantly the track for the topic whenever I needed it.

AUTOMATED TELLER MACHINE (ATM)

You're short on cash, so you walk over to the automated teller machine (ATM), insert your card into the card reader, respond to the prompts on the screen, and within a minute you walk away with your money and a receipt. These machines can now be found at most supermarkets, convenience storesand travel centers all over the country from coast to coast. But have you everwondered about the process that makes your bank funds available to you at any of the thousands of ATMs?

ATMs have become a quick, convenient way to access money inyour accounts.

Why ATM?

- International standard-based technology (for interoperability)
- Low network latency (for voice, video, and real-time applications)
- Low variance of delay (for voice and video transmission)
- Guaranteed quality of service
- High capacity switching (multi-giga bits per second)
- Bandwidth flexibility (dynamically assigned to users)
- Scalability (capacity may be increased on demand)

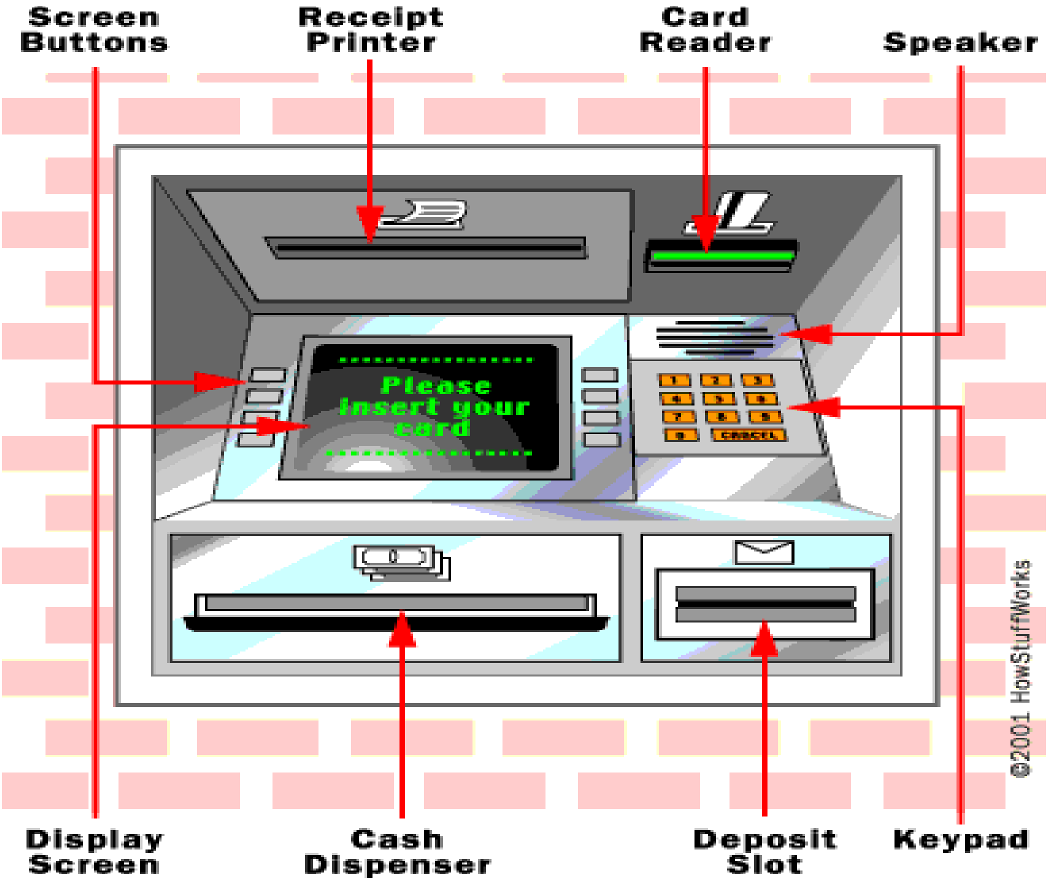
- Medium not shared for ATM LAN (no degradation in performance as trafficload or number of users increases)
- Supports a wide range of user access speeds
- Appropriate (seamless integration) for LANs, MANs, and WANs
- Supports audio, video, imagery, and data traffic (for integrated services)

PARTS OF THE MACHINE

You're probably one of the millions who has used an ATM. An ATM has following devices:

- CARD READER - The card reader captures the account information stored on the magnetic stripe on the back of an ATM/debit or credit card.The host processor uses this information to route the transaction to the cardholder's bank.

- KEYPAD - The key pad lets the cardholder tell the bank what kind of transaction is required (cash withdrawal, balance inquiry, etc.) and for what amount. Also, the bank requires the cardholder's personal identification number (PIN) for verification. Federal law requires that thePIN block be sent to the host processor in encrypted form.



- SPEAKER - The speaker provides the cardholder with tactile feedback when a key is pressed.

- DISPLAY SCREEN - The display screen prompts the cardholder through each step of the transaction process. Leased-line machines commonly use a monochrome or color CRT (cathode ray tube) display. Dial-up machines commonly use a monochrome or color LCD.

- RECEIPT PRINTER - The receipt printer provides the cardholder with a paper receipt of the transaction.

- CASH DISPENSER - The heart of an ATM is the safe and cash- dispensing mechanism. The entire bottom portion of most small ATMs is asafe that contains the cash.

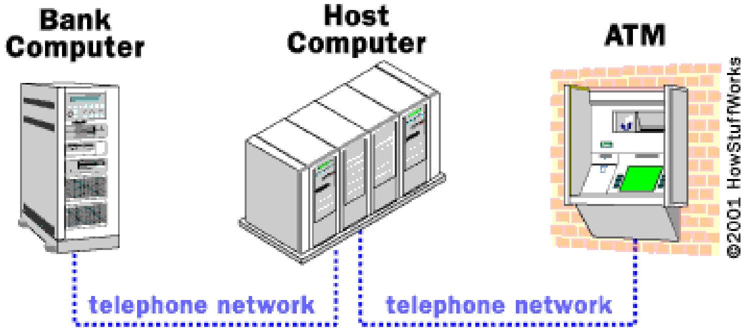
The cash-dispensing mechanism has an electric eye that counts each bill as it exits the dispenser. The bill count and all of the information pertaining to a particular transaction is recorded in a journal. The journal information is printed out periodically and a hard copy is maintained by the machine ownerfor two years. Whenever a cardholder has a dispute about a transaction, he orshe can ask for a journal printout showing the transaction, and then contact the host processor. If no one is available to provide the journal printout, the cardholder needs to notify the bank or institution that issued the card and fill out a form that will be faxed to the host processor. It is the host processor's responsibility to resolve the dispute.

Besides the electric eye that counts each bill, the cash-dispensing mechanismalso has a sensor that evaluates the thickness of each bill. If two bills are stuck together, then instead of being dispensed to the cardholder they are diverted to a reject bin. The same thing happens with a bill that is excessively worn or torn, or is folded.

The number of reject bills is also recorded so that the machine owner can be aware of the quality of bills that are being loaded into the machine. A high reject rate would indicate a problem with the bills or with the dispenser mechanism.

WORKING OF ATM

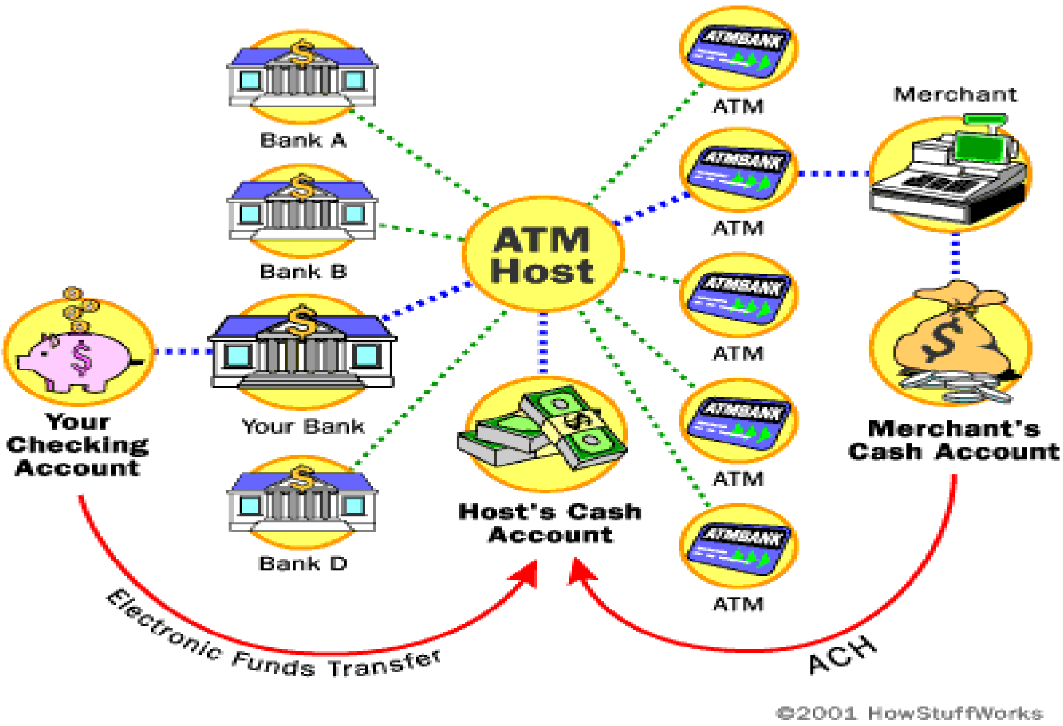
An ATM is simply a data terminal with two input and four output devices. Like any other data terminal, the ATM has to connect to, and communicatethrough, a host processor. The host processor is analogous to an internet service provider(ISP) in that it is the gateway through which all the variousATM networks become available to the cardholder (the person wanting thecash).



Most host processors can support either leased-line or dial-up machines. Leased-line machines connect directly to the host processor through a four-wire, point-to-point, dedicated telephone line. Dial-up ATMs connect to thehost processor through a normal phone line using a modem and a toll-free number, or through an Internet service provider using a local access numbervia a modem.

Leased-line ATMs are preferred for very high-volume locations because of their thru-put capability, and dial-up ATMs are preferred for retail merchantlocations where cost is a greater factor than thru-put. The initial cost for a dial-up machine is less than half that for a leased-line machine. The monthlyoperating costs for dial-up are only a fraction of the costs for leased line.

When a cardholder wants to do an ATM transaction, he or she provides the necessary information by means of the card reader and keypad. The ATM forwards this information to the host processor, which routes the transaction request to the cardholder's bank or institution that issued the card. If the cardholder is requesting cash, the host processor causes an electronic funds transfer to take place from the customer's checking account to the host processor's account. Once the funds are transferred to the host processor's bank account, the processor sends an approval code to the ATM authorizingthe machine to dispense the cash. The processor then ACHs the cardholder'sfunds into the merchant's bank account, usually the next bank business day. In this way, the merchant is reimbursed for all funds dispensed by the ATM.



An independent ATM host can access any bank. It also supports a largenumber of ATM's placed with different merchants.

So when you request cash, the money moves electronically from your account to the host's account to the merchant's account.

CREDIT CARDS

A BIT OF HISTORY

According to the Encyclopedia Britannica, the use of credit cards originatedin the **United States** during the **1920s**, when individual companies, such as hotel chains and oil companies, began issuing them to customers for purchases made at those businesses. This use increased significantly afterWorld War II.

The **first universal credit card** -- one that could be used at a variety of stores and businesses -- was introduced by **Diners club** ,inc. in **1950**. With this system, the credit-card company charged cardholders an annual fee andbilled them on a monthly or yearly basis. Another major universal card -- **"Don't leave home without it!"** -- was established in **1958** by the **American Express company.**

Later came the bank credit-card system. Under this plan, the bank credits the account of the merchant as sales slips are received (this meant merchants were paid quickly -- something they loved!) and assembles charges to be billed to the cardholder at the end of the billing period. The cardholder, in turn, pays the bank either the entire balance or in monthly installments with interest (sometimes called carrying charges).

The **first national bank plan** was **Bank Americard**, which was started on a statewide basis in **1959** by **the Bank of America in California**. This system was licensed in other states starting in 1966, and was renamed **Visa** in 1976.

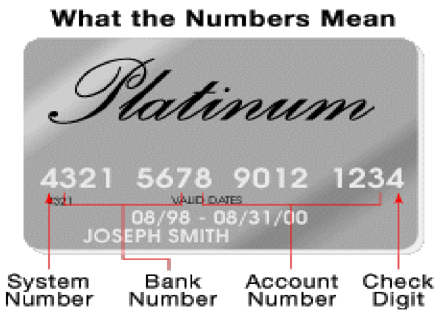
Other major bank cards followed, including **Master card**, formerly Master Charge. In order to offer expanded services, such as meals and lodging, many smaller banks that earlier offered credit cards on a local or regional basis formed relationships with large national or international banks.

STRUCTURE OF CARD

A credit card is a thin plastic card, usually **3-1/8 inches** by **2-1/8 inches** in size, that contains identification information such as a signature or picture, and authorizes the person named on it to charge purchases or services to hisaccount -- charges for which he will be billed periodically. Today, the information on the card is read by automated teller machines (ATMs), storereaders, and bank and Internet computers.

FRONT SIDE

Front side of every card have a unique number. Although phone , gas and department stores have their own numbering systems, **ANSI Standard X4.13-1983** is the system used by most national credit-card systems.



The front of your credit card has a lot of numbers -- here's an example of what they might mean.

Some of the numbers stand for:

The **first digit** in your credit-card number signifies the system :

- **3 - travel/entertainment cards (such as American Express and Diners Club)**
- **4 - Visa**
- **5 - Master card**
- **6 – Discover card**

The structure of the card number varies by system. For example, American Express card numbers start with 37; Carte Blanche and Diners Club with 38.

- **American Express** - Digits three and four are type and currency, digits five through 11 are the account number, digits 12 through 14 arethe card number within the account and digit 15 is a check digit.

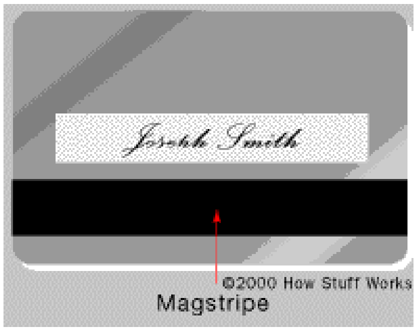
- **Visa** - Digits two through six are the bank number, digits seven through 12 or seven through 15 are the account number and digit 13 or 16is a check digit.

- **MasterCard** - Digits two and three, two through four, two through five or two through six are the bank number (depending on whether digit two is a 1, 2, 3 or other). The digits after the bank number up through digit15 are the account number, and digit 16 is a check digit.

BACK SIDE

The stripe on the back of a credit card is a magnetic stripe, often called a **magstripe.** The magstripe is made up of tiny **iron based magnetic** particlesin a

plastic-like film. Each particle is really a tiny bar magnet about 20- millionths of an inch long.



Your card has a magstripe on the back and a place for your all-important signature.The magstripe can be "written" because the tiny bar magnets can be magnetized in either a north or south pole direction. The magstripe on theback of the card is very similar to a piece of cassette tape.A magstripe readercan understand the information on the three-track stripe.

INFORMATION ON THE STRIPE

There are **three tracks** on the magstripe. Each track is about one-tenth of aninch wide. **The ISO/IEC standard 7811**, which is used by banks, specifies:

- Track one is **210 bits** per inch (bpi), and holds 79 6-bit plus parity bit read-only characters.
- Track two is **75 bpi**, and holds 40 4-bit plus parity bit characters.
- Track three is **210 bpi**, and holds 107 4-bit plus parity bit characters.

Your credit card typically uses only tracks one and two. Track three is a read/write track (which includes an encrypted PIN, country code, currency units and amount authorized), but its usage is not standardized among banks.

The information on **track one** is contained in two formats: A, which is reserved for proprietary use of the card issuer, and B, which includes the following:

- **Start sentinel - one character**
- **Format code="B" - one character (alpha only)**
- **Primary account number - up to 19 characters**
- **Separator - one character**
- **Country code - three characters**
- **Name - two to 26 characters**
- **Separator - one character**
- **Expiration date or separator - four characters or one character**
- **Discretionary data - enough characters to fill out maximum record length (79 characters total)**
- **End sentinel - one character**
- **Longitudinal redundancy check (LRC) - one character**

  LRC is a form of computed check character.

The format for **track two**, developed by the banking industry, is as follows:

- **Start sentinel - one character**
- **Primary account number - up to 19 characters**
- **Separator - one character**
- **Country code - three characters**
- **Expiration date or separator - four characters or one character**
- **Discretionary data - enough characters to fill out maximum record length (40 characters total)**
- **LRC - one character**

If the ATM isn't accepting your card, your problem is probably either:

- A dirty or scratched magstripe

- An erased magstripe (The most common causes for erased magstripes are exposure to magnets)

TYPES OF CARDS

There are basically three types of credit cards:

- **Bank cards**, issued by banks (for example, Visa, MasterCard and Discover Card)

- **Travel and entertainment (T&E) cards**, such as American Express and Diners Club

- House cards that are good only in one chain of stores (**Sears** is the biggestone of these, followed by the oil companies, phone companies and local department stores.)

ATM CARD VS. CHECK CARD

As an alternative to writing checks and using a credit cards, most major banks have teamed up with major credit-card companies to issue check cards.

Check cards are different from straight ATM cards in a couple of ways. First, check cards are also known as debit cards because of how they work --instead of getting credit for your purchase and receiving a monthly bill, like you do with a credit card, a check/debit card deducts money from your checking or savings account.

Also, while you can only use your ATM card at the ATM machine (and some grocery stores), you can use a check card at any retailer that accepts credit cards, such as:

- Grocery stores
- Gas stations
- Discount superstores
- Book stores
- Ticket counters (concert tickets, airline tickets, etc.)
- Pharmacies
- Hotels
- E-tailers
- Restaurants

ATM cards and check cards can be used in different ways.

You can use your check card as a either credit card or a debit card -- either way, it comes out of your account. The only difference is that if you tell theclerk "credit card," you sign a slip, and if tell the clerk "debit card," you enter your PIN number instead of signing.

It's easy to tell the difference between a plain ATM card and a check card: A check card has your name, "credit" account number, the credit company's logo, the bank's logo and "Check Card" printed across the front of it; an ATM card has only your name, account number and bank's logo on the frontof it. Both cards have strips on the back for the authorized cardholder to signon. A check card company, such as visa, has agreements with banks to issuewhat looks like a Visa credit card. A Visa check card can be used at any retailer that accepts Visa credit cards and at ATMs worldwide.

How E-ZPass Works

You never want to be stuck on a toll road without a pocket full of change. Itcan be a bit nerve-racking to dig through the car seats, trying to find something to give to the toll booth attendant while drivers behind you honkand yell for you to move on. These are the kinds of situations that cause delays at toll plazas.

Toll plazas like this one are familiar sites to millions of drivers.

Today, most toll roads are equipped with an electronic toll-collection system, like E-ZPass, that detects and processes tolls electronically. E-ZPassis used by several U.S. states, but most other electronic toll systems are verysimilar to E-ZPass. Basically, E-ZPass uses a vehicle-mounted transponder that is activated by an antenna on a toll lane. Your account information is stored in the transponder. The antenna identifies your transponder and reads your account information. The amount of the toll is deducted and you're allowed through.

Electronic toll collection is designed to make traffic flow faster, as cars don't have to stop to make a transaction.

The Basics

Millions of drivers pass through toll booths every day. Traditionally, the process is to put some change in a basket, which tabulates the coins and opens a gate to allow the driver through. Today, many local and state trafficagencies have installed or are installing electronic readers that allow driversto pass through toll stations without coming to a complete stop. The names of the systems vary, but they all work in pretty much the same way.

Motorists can drive through E-ZPass toll lanes without stopping.

Here are the basic components that make the system work:

- Transponder
- Antenna
- Lane controller - This is the computer that controls the lane equipmentand tracks vehicles passing through. It is networked on a Local area network (LAN).
- Host computer system - All of the toll plaza LANs are connected to a central database via a Wide area network (WAN).

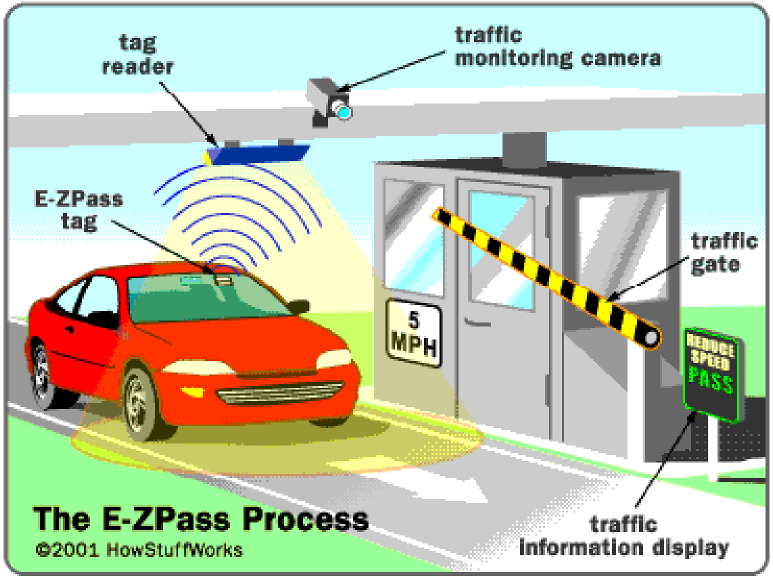
Drivers usually have to pay a deposit to obtain a transponder, which is aboutthe size of a deck of cards. This device is placed on the inside of the car's windshield behind the rearview mirror. A transponder is a battery-operated, radio frequency identification (RFID) unit that transmits radio signals. The transponder is a two-way radio with a microprocessor, operating in the 900-MHz band. Stored in this RFID transponder is some basic account information, such as an identification number.

Antennas, or electronic readers, are positioned above each toll lane. These antennas emit radio frequencies that communicate with the transponder. The detection zone of an antenna is typically 6 to 10 feet (2 to 3 m) wide and about

10 feet long. These two devices, the transponder and the antenna, interact to complete the toll transaction.

Some electronic toll-collection systems may also include a light curtain and treadles. A light curtain is just a beam of light that is directed across the lane. When that beam of light is broken, the system knows a car has entered. Treadles are sensor strips embedded in the road that detect the number of axles a vehicle has. A three-axle vehicle is charged a higher toll than a two- axle vehicle. These two devices are safeguards to ensure that all vehicles arecounted correctly.

No Change, No Problem By installing electronic toll-collection systems, government agencies believe that traffic will move faster. The idea is that even if commuters have to slow down for the toll booths, they can get through faster with a system like E-ZPass. Motorists no longer have to worryabout stopping to deposit or hand over the toll -- and there is certainly no searching the car for loose change. As long as they've paid on their E-ZPass account, they just have to rely on the lane antenna to read the signals from the transponder.



Here's how the system works:

- As a car approaches a toll plaza, the radio-frequency (RF) field emitted from the antenna activates the transponder.
- The transponder broadcasts a signal back to the lane antenna with some basic information.

- That information is transferred from the lane antenna to the central database.
- If the account is in good standing, a toll is deducted from the driver's prepaid account.
- If the toll lane has a gate, the gate opens.
- A green light indicates that the driver can proceed. Some lanes have text messages that inform drivers of the toll just paid and their accountbalance.

The entire process takes a matter of seconds to complete. The electronic system records each toll transaction, including the time, date, plaza and toll charge of each vehicle. Typically, consumers maintain prepaid accounts. A yellow light or some other signal will flash to indicate if an account is low ordepleted.

The rules regarding how fast you can pass through the toll plaza vary fromsystem to system. Some traffic agencies allow drivers to pass through the system at 55 miles per hour (86 kph). Others want you to slow down to 30mph (48 kph), or even 5 mph (8 kph).

These lanes are monitored using video cameras. Some states allow cars to drive right through the toll plaza as the antenna detects the transponder. Ifyou try to go through the plaza without a transponder, the camera recordsyou and takes a snapshot of your license plate. The vehicle owner then receives a violation notice in the mail.

How Encryption Works

Information security is provided on computers and over the Internet by a variety of methods. A simple but straightforward security method is to onlykeep sensitive information on removable storage media like floppy disks.
But the most popular forms of security all rely on encryption, the process of encoding information in such a way that only the person (or computer) with the key can decode it.

Computer encryption is based on the science of cryptography, which has been used throughout history. Before the digital age, the biggest users of cryptography were governments, particularly for military purposes. The existence of coded messages has been verified as far back as the Roman Empire. But most forms of cryptography in use these days rely on computers, simply because a human-based code is too easy for a computer tocrack.

Most computer encryption systems belong in one of two categories:

- Symmetric-key encryption
- Public-key encryption

Symmetric Key

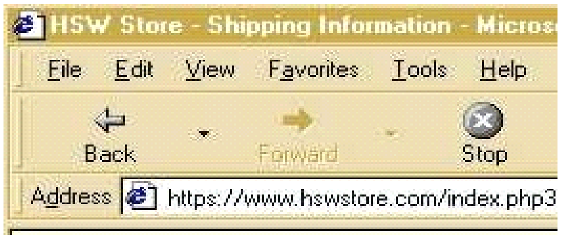
In symmetric-key encryption, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the networkto another computer. Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one. Symmetric-key encryption is essentially the same as a secret code thateach of the two computers must know in order to decode the information.
The code provides the key to decoding the message. Think of it like this: You create a coded message to send to a friend in which each letter is substituted with the letter that is two down from it in the alphabet. So "A" becomes "C," and "B" becomes "D". You have already told a trusted friendthat the code is "Shift by 2". Your friend gets the message and decodes it. Anyone else who sees the message will see only nonsense.

Public Key

Public-key encryption uses a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key. Avery popular public-key encryption utility is called Pretty Good Privacy (PGP), which allows you to encrypt almost anything. You can find out moreabout PGP at the PGP site.

To implement public-key encryption on a large scale, such as a secure Web server might need, requires a different approach. This is where digital certificates come in. A digital certificate is basically a bit of information thatsays that the Web server is trusted by an independent source known as a certificate authority. The certificate authority acts as a middleman that both computers trust. It confirms that each computer is in fact who it says it is, and then provides the public keys of each computer to the other.

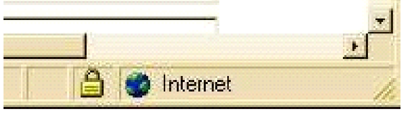
A popular implementation of public-key encryption is the Secure Sockets Layer (SSL). Originally developed by Netscape, SSL is an Internet security protocol used by Internet browsers and Web servers to transmit sensitive information. SSL recently became part of an overall security protocol knownas Transport Layer Security (TLS).


HSW Store - Shipping Information - Micros

Address https://www.hswstore.com/index.php3

Look for the "s" after "http" in the address whenever you are about to enter sensitive information, such as a credit-card number, into a form on a Web site.

In your browser, you can tell when you are using a secure protocol, such as TLS, in a couple of different ways. You will notice that the "http" in the address line is replaced with "https," and you should see a small padlock inthe status bar at the bottom of the browser window.



The padlock symbol lets you know that you are using encryption.

Public-key encryption takes a lot of computing, so most systems use a combination of public-key and symmetry. When two computers initiate a secure session, one computer creates a symmetric key and sends it to the other computer using public-key encryption. The two computers can then communicate using symmetric-key encryption. Once the session is finished,each computer discards the symmetric key used for that session. Any additional sessions require that a new symmetric key be created, and the process is repeated.

Are You Authentic?As stated earlier, encryption is the process of taking all of the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Another process, authentication, is used to verify that the information comes from a trusted source. Basically, if information is "authentic," you know who created it andyou know that it has not been altered in any way since that person created it.These two processes, encryption and authentication, work hand-in-hand to create a secure environment.

There are several ways to authenticate a person or information on acomputer:

- Password - The use of a user name and password provides the most common form of authentication. You enter your name and password when prompted by the computer. It checks the pair against a secure file to confirm. If either the name or the password does not match, then you are not allowed further access.
- Pass cards - These cards can range from a simple card with a magnetic strip, similar to a credit card, to sophisticated smart cards that have an embedded computer chip.
- Digital signatures - A digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file) is authentic. The Digital Signature Standard (DSS) is based on a type ofpublic-key encryption method that uses the Digital Signature Algorithm (DSA). DSS is the format for digital signatures that has been endorsed by the U.S. government. The DSA algorithm consists of a private key, known only by the originator of the document (the signer), and a public key. The public key has four parts, which you can learn more about at this page. If anything at all is changed in the document after the digital signature is attached to it, it changes the value that the digital signature compares to, rendering the signature invalid.

Recently, more sophisticated forms of authentication have begun to show upon home and office computer systems. Most of these new systems use someform of biometrics for authentication. Biometrics uses biological information to verify identity. Biometric authentication methods include:

- Fingerprint scan
- Retina scan
- Face scan
- Voice identification

Another secure-computing need is to ensure that the data has not been corrupted during transmission or encryption. There are a couple of popular ways to do this:

- Checksum - Probably one of the oldest methods of ensuring that data is correct, checksums also provide a form of authentication because an invalid checksum suggests that the data has been compromised in some fashion. A checksum is determined in one of two ways. Let's saythe checksum of a packet is 1 byte long. A byte is made up of 8 bits, and each bit can be in one of two states, leading to a total of 256 (2^8) possible combinations. Since the first combination equals zero, a byte can have a maximum value of 255.
    - If the sum of the other bytes in the packet is 255 or less, thenthe checksum contains that exact value.
    - If the sum of the other bytes is more than 255, then the checksum is the remainder of the total value after it has been divided by 256.

Let's look at a checksum example:

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Total	Checksum
212	232	54	135	244	15	179	80	1,151	127

- 1,151 / 256 = 4.496 (round to 4)
- 4 x 256 = 1,024
- 1,151 - 1,024 = 127

- Cyclic Redundancy Check (CRC) - CRCs are similar in concept to checksums, but they use polynomial division to determine the value ofthe CRC, which is usually 16 or 32 bits in length. The good thing about CRC is that it is very accurate. If a single bit is incorrect, the CRC value will not match up. Both checksum and CRC are good for preventing random errors in transmission but provide little protection from an intentional attack on your data. Symmetric- and public-key encryption techniques are much more secure.

All of these various processes combine to provide you with the tools you need to ensure that the information you send or receive over the Internet is secure. In fact, sending information over a computer network is often much more secure than sending it any other way. Phones, especially cordless phones, are susceptible to eavesdropping, particularly by unscrupulous people with radio scanners. Traditional mail and other physical mediums often pass through numerous hands on the way to their destination, increasing the possibility of corruption. Understanding encryption, and simply making sure that any sensitive information you send over the Internetis secure (remember the "https" and padlock symbol), can provide you with greater peace of mind.

SMART CARDS The "smart" credit card is an innovative application that involves all aspects of cryptography (secret codes), not just the authentication we described in the last section. A Smart Card has a microprocessor built into the card itself. Cryptography is essential to the functioning of these cards in several ways:

- The user must corroborate his identity to the card each time a transaction is made, in much the same way that a PIN is used with anATM.
- The card and the card reader execute a sequence of encrypted sign/countersign-like exchanges to verify that each is dealing with a legitimate counterpart.
- Once this has been established, the transaction itself is carried out in encrypted form to prevent anyone, including the cardholder or the merchant whose card reader is involved, from "eavesdropping" on the exchange and later impersonating either party to defraud the system.

This elaborate protocol is conducted in such a way that it is invisible to theuser, except for the necessity of entering a PIN to begin the transaction.

Smart cards first saw general use in France in 1984. They are now hot commodities that are expected to replace the simple plastic cards most of ususe now. Visa and MasterCard are leading the way in the United States withtheir Smart Card technologies.

The chips in these cards are capable of many kinds of transactions. For example, you could make purchases from your credit account, debit account or from a stored account value that's reloadable. The enhanced memory and processing capacity of the Smart Card is many times that of traditional magnetic-stripe cards and can accommodate several different applications ona single card. It can also hold identification information, keep track of your participation in an affinity (loyalty) program or provide access to your office. This means no more shuffling through cards in your wallet to find theright one -- the Smart Card will be the only one you need!

New Innovations

Several companies are designing ATMs for the blind. These machines wouldbe located at kiosks rather than bank drive-thrus. For several years, the keypads at ATMs were equipped with braille for the blind or visually impaired.

New innovations in this technology will include machines that will verbally prompt the customer for their card, their PIN and what type of transaction they would like.

ATM Security

Many banks recommend that you select your own personal identificationnumber (PIN).

Visa recommends the following PIN tips:

- Don't write down your PIN. If you must write it down, do not store itin your wallet or purse.

- Make your PIN a series of letters or numbers that you can easily remember, but that cannot easily be associated with you personally.

- Avoid using birth dates, initials, house numbers or your phone number.

Visa also recommends the following tips for safe ATM usage:

- Store your ATM card in your purse or wallet, in an area where it won'tget scratched or bent.
- Get your card out BEFORE you approach the ATM. You'll be more vulnerable to attack if you're standing in front of the ATM, fumbling through your wallet for your card.
- Stand directly in front of the ATM keypad when typing in your PIN.This prevents anyone waiting to use the machine from seeing your personal information.
- After your transaction, take your receipt, card and money away. Donot stand in front of the machine and count your money.
- If you are using a drive-up ATM, get your vehicle as close to the machine as possible to prevent anyone from coming up to your window. Also make sure that your doors are locked before you driveup to the machine.
- Do not leave your car running while using a walk-up ATM. Take your keys with you and lock the doors before your transaction.
- If someone or something makes you uncomfortable, cancel your transaction and leave the machine immediately. Follow up with your bank to make sure the transaction was cancelled and alert them to any suspicious people.

Many retail merchants close their store at night. It is strongly recommendedthat they pull the money out of the machine when they close, just like they do with their cash registers, and leave the door to the security compartment

wide open like they do with an empty cash-register drawer. This makes it obvious to any would-be thief that this not payday.

It's important to use a well-lit, public ATM machine at night.

For safety reasons, ATM users should seek out a machine that is located in a well-lighted public place. Federal law requires that only the last four digits of the cardholder's account number be printed on the transaction receipt so that when a receipt is left at the machine location, the account number is secure. However, the entry of your four-digit personal identification number(PIN) on the keypad should still be obscured from observation, which can bedone by positioning your hand and body in such a way that the PIN entry cannot be recorded by store cameras or store employees. The cardholder's PIN is not recorded in the journal, but the account number is. If you protect your PIN, you protect your account.

Your ATM PIN should be a number that you could easily remember, butthat would not be readily-available to thieves.

Reference

- www.google.com
- www.wikipedia.org

- www.studymafia.org