TECHNOLOGY SOLUTIONS

- There are two lines of defense of e-commerce security: technology solutions and policy solutions.
- PROTECTING INTERNET COMMUNICATION
- E-commerce transactions must flow over the public Internet, involving thousands of routers and servers through which the transaction packet flows. Security expert believe the greatest security threat occur at the level of Internet communications.
- However, a number of tools are available to protect the security of Internet communications, the most basic of which is message encryption.

Technology Solution Cont.

- The following are tools available to achieve site security:
  - Encryption
  - Firewalls
  - Security tools
  - Network security protocols
  - Virtual private networks
  - Tunneling
  - Access controls
  - Authentication
  - Instruction detection
  - Proxy/agent systems
  - Security management

Encryption

- Encryption is the process of transforming plain text or data into **cipher text** that cannot be read by anyone other than the sender and the receiver.
- The purpose of encryption is
  - to secure stored information and
  - to secure information transmission
- Encryption can provide four of the six dimensions of e-commerce security earlier discussed.
  - Message integrity – provides assurance that the message has not been altered.
  - Nonrepudiation – prevents the user from denying he or she sent the message.

Encryption Cont.

  - Authentication – provides verification of the identity of the person or computer sending the message.
  - Confidentiality – gives assurance that the message was nor read by anyone.
- The transformation of plain text to cipher text is accomplished by using a key or cipher. A key or cipher is any method for transforming plain text to cipher text.
- Encryption has been in existence and used since the earliest form of writing and commercial transactions. Ancient Egyptian commercial records were encrypted using substitution and transposition ciphers.

Encryption Cont.

- In a **substitution cipher**, every occurrence of a given letter is replaced systematically by another letter. For instance, if we used the cipher “letter plus two” – meaning replace every letter in a word with a new letter two places forward – the word “Hello” in plain text would be transformed into the following cipher text: JGNNQ”.

- In a **transposition cipher,** the ordering of the letters in each word is changed in some systematic way. The word “Hello” can be written backward as “OLLEH”. A complicated cipher would (a) break all words into two and (b) spell the first word with every other letter beginning with first letter, and then spell the second word with the all the remaining letters. In this cipher, “HELLO” would be written as “HLO EL.”

Encryption Cont.

Symmetric Key Encryption

- In order to decipher these messages, the receiver would have to know the secret cipher that was used to encrypt the plain text. This is called symmetric key encryption or secret key encryption.
- In symmetric key encryption, both the sender and receiver use the same key to encrypt and decrypt the message. The sender and receiver receive the key over some communication channels or exchange the key in person. Symmetric key encryption was used extensively during War II and currently part of Internet encryption.

Encryption Cont.

- The possibilities for simple substitution and transposition ciphers are endless, but they all suffer from common flaws.
- First, in the digital age, computers are so powerful and fast that the ancient means of encryption can be broken quickly.
- Second, symmetric key encryption requires that both parties share the same key. In order to share the same key, they must be sent over a presumably insecure medium where it could be stolen.
- Third, in commercial use, you will need a secret key for all the parties involved. Where you have thousand or million customers it becomes impossible to keep all the secret keys.

Encryption Cont.

- Modern encryption systems are digital. The keys or ciphers used in transforming the plain text into cipher text are digital strings composed of 0s and 1s. For example, ASCII representation of letter ‘A’ accomplished with eight binary digits is 01000001.
- One way in which digital strings can be transformed in cipher text is by multiplying each letter by another eight-bit key number 0101 0101.
- If we multiply every digital character in our text messages by this eight-bit key, sent the encrypted message to a friend along with the secret eight-bit key, the friend decode the message easily.

Encryption Cont.

- The strength security protection is measured by the length of the binary key used to encrypt the data. With eight-bit key earlier mention can easily be broken by intruder because there are only 2^8 or 256 possibilities.
- Modern digital encryption use keys with 56, 128, 256, or 512 binary digits. With encryption keys of 512 digits, it is estimated that all the computers in the world need to work for 10 years before breaking into the answer.
- The **Data Encryption Standard (DES)** was developed by National Security Agency (NSA) and IBM in the 1950s. DES uses a 56-bit encryption key. It had been improved over the years. Presently, the most common symmetric encryption algorithm is **Advance Encryption Standard (AES)**, which offers key sizes of 128, 192, and 256 bits. There are also many other symmetric key systems with keys up to 2048 bits.

Encryption Cont.

Public key Encryption

- In 1976, a new way of encrypting messages called **public key cryptography** was invented by Whitefield Diffie and Martin Hellman. Public key cryptography solves the problems of exchanges keys. In this method, two mathematically related digital keys are used: a public key and private key.
- The private is kept secret by the owner, and the public key is widely disseminated. Both can be used to encrypt and decrypt the messages. However, once the keys are used to encrypt a message, that same key cannot be used to unencrypt the message.
- The mathematical algorithms used to produce the key are one-way function. Public key cryptography is based on irreversible mathematical functions. The keys are long (128, 256 and 512-bit keys) that would take great computing power to obtain one key from other using the largest and fastest computer available.

Encryption Cont.

Public Key Cryptography –Illustrated with a simple case	
Step	Description
1. The sender creates a digital message.	The message could be a text, spreadsheet or any digital object.
2. The sender obtains the recipient's public key from a public directory and applies it to the message.	Public keys are public widely and can be obtained from recipients directly.
3. Application of the recipient's key produces an encrypted ciphertext message.	Once encrypted using the public key the message cannot be unencrypted with the same public key.
4. The encrypted message is sent over the Internet.	The encrypted message is broken into packets and sent through several different pathways, making interception practically impossible.
5. The recipient uses his/her private key to decrypt the message.	The only person who can decrypt the message is the person who possess the recipient's private key.

Encryption

Public Key Encryption Using Digital Signature and Hash Digests

- In public key encryption, some important features of security are missing. Although the message sent can be guaranteed that it was not accessed by third party (message confidentiality), there is no guarantee that the sender is really the sender because there is no authentication.
- This means the sender can deny ever sending any message (repudiation) and there is no assurance the message was not altered in transit. This point out lack of security in the public key encryption.
- A more sophisticated public key cryptography can achieve authentication, nonrepudiation, and integrity.

Encryption Cont.

- A hash function is used to check the confidentiality of the message and ensure the message is not altered in transit. A hash function is an algorithm that produces a fixed-length number called a hash or message digest. A hash function can count the number of 0s, 1s, 00s, 11s and so on. The more complex a hash function is, the more hashes or hash results are produced that are unique to every message.
- The result of the hash function is sent by the sender to the recipient. Upon receipt, the recipient applies the hash function to the received message and checks to verify the same results is produced. Same result, means the message has not been altered.
- The sender then encrypts both the hash result and the original message using the recipient's public key producing a single block of cipher text.

- To ensure the authenticity of the message and nonrepudiation of the message, the sender encrypts the entire block of cipher text one more time using the sender private key. This produces a **digital signature** also called *e-signature* or 'signed' cipher text that can be sent over the Internet.
- A digital signature is close to hand written signature because the private key is unique to individual. When the private key is used with hash function, the digital signature is even more unique than a hand written signature.

Encryption Cont.

- The recipient of this signed cipher text uses the sender's public key to authenticate the message. Once authenticated, the recipient uses his or her private key to obtain the hash result and the message.
- Finally, the recipient applies the same hash function to the original message and compares the result with result sent by the sender. If the same result is obtained, the recipient is sure that the message has not been altered during transmission. The message has integrity.

Public Key Cryptography with Digital Signature	
Step	Description
1. The sender creates an original message.	The message could be any digital file.
2. The sender applies a hash function, producing 128-bits hash result.	Hash function creates a unique digest of the message based on the message content.
3. The sender encrypts the message and hash result using recipient's public key.	This irreversible process creates a cipher text that can be read only by the recipient using his or her private key.
4. The sender encrypts the result, again using his or her private key	The sender private key is a digital signature. There is only person who create this digital mark.
5. The result of this double encryption is sent over the Internet.	The message traverses the Internet as a series of independent packet.
6. The receiver uses the sender's public key to authenticate the message.	Only person could send this message, namely the sender.
7. The receiver uses his or her private key to decrypt the hash function and the original message. The receiver checks to ensure the original message and the hash function results conform to one another.	The hash function is used here to check the original message. This ensure the message was not changed in transit.

Encryption Cont.

Digital Envelopes

- Public key encryption is computationally slow. Symmetric key encryption is computationally faster, but has a weakness of symmetric key must be sent to recipient over insecure transmission lines.
- An efficient way to provide a solution is to use symmetric key encryption and decryption for a large document and use the public key encryption to encrypt and send the symmetric key. This technique is called using a **digital envelope**.

Encryption Cont.

- For instance, a document is encrypted using a symmetric key. The symmetric key which the recipient will need to decrypt the document is also encrypted using the recipient's public key.
- The encrypted report and the digital envelopes are sent across the web. The recipient first use his or her private key to decrypt the symmetric key, and subsequently use the symmetric key to decrypt the report.
- This method saves time because both encryption and decryption are faster with symmetric key.

Encryption Cont.

Digital Certificates and Public Key Infrastructure (PKI)

- There is still some deficiencies in the message security earlier mentioned. How do we know that people and institutions are who they claim to be? People can make up a private and public key combination and claim to be someone they are not.
- When placing an order with online merchant such as Amazon.com, you really want to be sure that it is real Amazon and not a spoofer masquerading as Amazon.

Encryption Cont.

- Digital certificates and the supporting public key infrastructure, are an attempt to solve this problem of digital identity.
- **A digital certificate** is a digital document issued by a trusted third party institution known as a **certification authority (CA)** that contains the name of the subject or company, the subject's public key, a digital certificate serial number, an expiration date, an issuance date, the digital signature of the certification authority and other identifying information.
- Public key infrastructure (PKI) refers to the CAs and digital certificate procedures that are accepted by all parties.

Encryption Cont.

- There are several ways the certificates are used in commerce. Before initiating a transaction, the customer can request the signed digital certificate of the merchant and decrypt using the merchant's public key to obtain both the message digest and the certificate issued.
- If the message digest matches the certificate, then the merchant and the public key are authenticated. The merchant may in turn request certification of the user, in which case the user would send the merchant his or her individual certificate.
- There are many types of certificates: personal, institutional, web server, software publisher, and CAs themselves.