Secure Data Storage

Cryptology

- Origin of encryption
- First instances believed to be Scytale (Wikipedia)
  - Wrap strip of paper (or maybe hide) around a stick, and write message along stick length. When paper is unraveled, the message becomes illegible.

Types of Encryption

- Classic ciphers, including substitution and transposition
- Good dog: PLLX XLP
  - L for o, p for g, x for d
- Good dog: dgogdoo - transpose letters
- Polyalphabetic, uses a substitution cipher, but with multiple instances of the alphabet. One example is the tabula recta; a table of the alphabet with each row off-set by one letter (Wikipedia)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Types of Encryption

- Mechanical encryption - early 20th century encryption and decryption using machines that would transpose, use polyaphabetic substitution, and possibly other substitutions, using rotor disks and plug board wires. Changing the disks and wires changed ciphers.
- Modern encryption can be divided into two types - symmetric key algorithms and asymmetric key algorithms.

Keys

- In cryptology, a key is a piece of information that controls the operation of the cryptographic process (algorithm)
- Specifically translates plaintext to ciphertext, or vice versa
- Come in different sizes, although 256 bit keys are considered very strong
- Can also be used in digital signatures and message authentication codes

Symmetric Key Algorithm

- Sender and receiver have a shared key, often identical key. Key should be kept secret
- Other terms for symmetric-key encryption are secret-key, single-key, one-key and eventually private-key encryption
  - The term private-key encryption, when discussing symmetric keys, can be confused with private key/public key cryptography in asymmetric key algorithms, and should be avoided

Data Encryption Standard

- DES was the standard for data encryption in the US
  - In 1976, US government selected DES believing it was too complex to be cracked. Early estimates indicated a $20M computer would be needed to crack
  - Uses a 56 bit key to encrypt the data (64 bit block with 8 bits for parity)

Triple DES

- TDES or 3DES replaced DES, given its susceptibility to hacking
- Has key size 3 times DES, with parity, allowing for 192 bit theoretical key size.
  - 3DES is susceptible to Man in the Middle attack, limiting its overall real world key size to 112 bits
- Also fading from use, being replaced by AES
  - DES and 3DES suffer from performance issues

Advanced Encryption Standard

- Also known as Rijndael (but technically isn't)
- AES is the new standard adopted by US gov’t
- One of the more, if not most popular encryption symmetric standard
- Uses fixed data block size of 128 bits and a key size of 128, 192, or 256 bits.
- http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Asymmetric Key Algorithms

- Often called public key cryptology
- Uses two keys, one available publicly, one privately used to decode the data
- Requires distribution of public key when it is updated/renewed. Requires revoking of old/stale public keys
  - Can lead to potential problems
- Example would be RSA, SSL (TLS)

Hashing

- Another type of encryption is one way encryption, or hashing, where the resulting encrypted string isn't expected to be decrypted
- Often used for password or passphrase storage
  - Without a way to decrypt a password, the password should be more secure, however, bad passwords weaken this benefit

Hashing

- The process for using hashing often works like this:
  - User supplies a plaintext string
  - A unique string is generated, called a salt, and is used with the plaintext string
  - The strings are then encrypted using an algorithm that doesn't allow for unencryption
  - The hash and the salt are stored, often together, in some kind of tabular form. Sometimes other support data (algorithm, cost) are also stored.

Transport Layer Security

- Formally known as Secure Socket Layer (SSL)
- New standard for many web communications
- Requires three phases:
  1. Peer negotiation for algorithm support
  2. Public key exchange and certificate-based authentication
  3. Symmetric cipher encryption

How TLS works (from Wikipedia)

- A TLS client and server negotiate a stateful connection by using a handshaking procedure. During this handshake, the client and server agree on various parameters used to establish the connection's security.
  - The handshake begins when a client connects to a TLS-enabled server requesting a secure connection, and presents a list of supported ciphers and hash functions.
  - From this list, the server picks the strongest cipher and hash function that it also supports and notifies the client of the decision.
  - The server sends back its identification in the form of a digital certificate. The certificate usually contains the server name, the trusted certificate authority (CA), and the server's public encryption key.

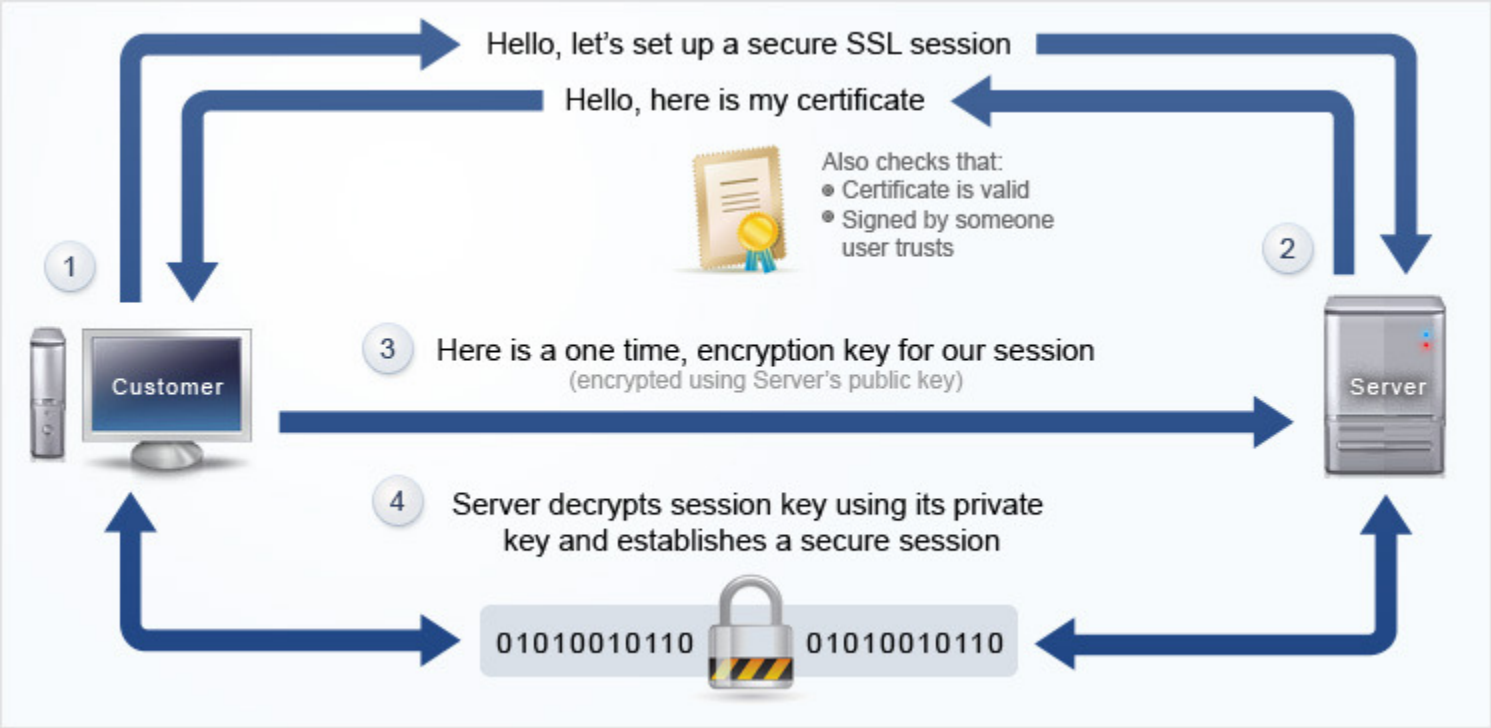
How TLS works (from Wikipedia)

- The client may contact the server that issued the certificate (the trusted CA as above) and confirm that the certificate is authentic before proceeding.
  - In order to generate the session keys used for the secure connection, the client encrypts a random number with the server's public key, and sends the result to the server. Only the server can decrypt it (with its private key): this is the one fact that makes the keys hidden from third parties, since only the server and the client have access to this data.
  - Both parties generate key material for encryption and decryption.

How TLS works (from Wikipedia)

- This concludes the handshake and begins the secured connection, which is encrypted and decrypted with the key material until the connection closes.
- If any one of the above steps fails, the TLS handshake fails, and the connection is not created.
- http://en.wikipedia.org/wiki/Secure_Socket_Layer

How TLS Works



Traffic Analysis

- Process of intercepting and examining messages to deduce information from patterns, specifically encrypted messages that cannot be decrypted.
- The more messages observed, intercepted, and/or stored, the greater the greater the likelihood of determining patterns from the traffic
- An example would be watching SSH traffic during login (Wikipedia)
- Man in the middle attacks – vulnerability for SSL

Uses

- Storage, network traffic, mobile phones, wireless devices, Bluetooth, ATMs, and DRM.
- Encryption of intellectual property in otherwise visible code (HTML, ASP, PHP)

Zend Guard (Encoder)

- https://www.zend.com/en/products/zend-guard

- Enables code protection via saving code in the closed “Zend Intermediate Code” format
  - Requires components installed on server
  - Requires PHP 4.2.x up to 5.0.x
- Other uses, including timed license and other license limitations.

HTML Guardian

- http://www.protware.com/

- Tools to protect HTML, JavaScript, PHP, ASP code.