



SECURITY

Cryptography

The Basic Idea:

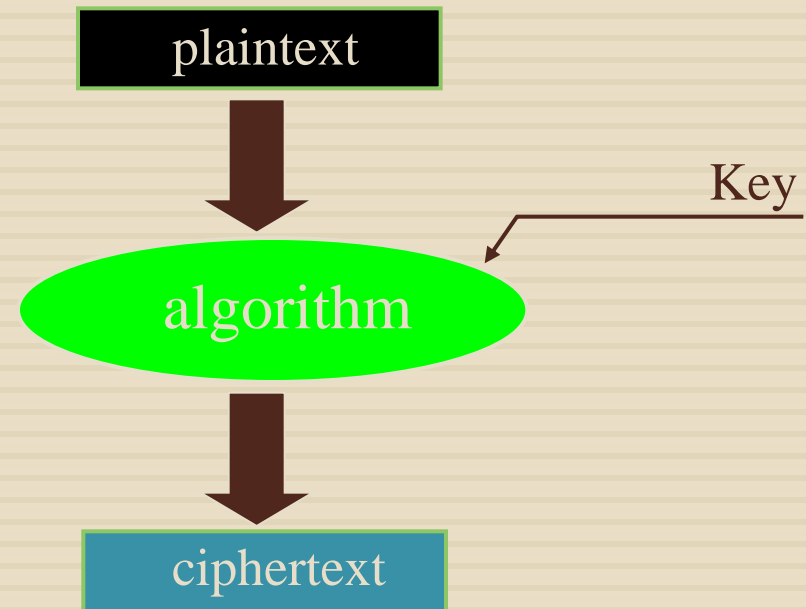
Two approaches:

- 1) ~~Make algorithm secret and don't use a key.~~

Bad Idea

- 2) Make algorithm public but keep the key secret.

Good Idea



Before Computers

Substitution ciphers ruled:

Caesar (Shift by N): 26 possibilities, easy to decode

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
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

Key Phrase: Lots of possibilities, a bit harder to decode

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

Random Mapping: 4×10^{26} possibilities, harder to decode

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

Before Computers

Cryptanalysis:

First known publication:

“A Manuscript on Deciphering Cryptographic Messages”

By the ninth century Arab scholar:

Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn 'omran ibn Ismail al-Kindi

Statistical “Frequency Analysis” of letters & words can easily break any mono-alphabetic substitution cipher.

In English: most common letters: E, T, A, O, I, N, S, ...

most common 2 letters words: ON, AS, TO, AT, IT...

most common 3 letters words: THE, AND, FOR, WAS,...

Vigenere square (1586)

	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Vigenere square

	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Keyword VOTEVOTEVOTEVOTEVOTE...

Plaintext ihavethreestinkydogs...

Ciphertext DVTZZHAVZSLXDBDCYCZW...

← Immune to frequency analysis !



However:

IF

If the key is as long as the message

AND

The key is completely random

THEN

The encryption is perfect (can't be broken) !!!

This is an example of Symmetric Key Encryption

Plaintext	DEAD		1101	1110	1010	1101	
Key	BEEF	\oplus	1011	1110	1110	1111	
Ciphertext		=	0110	0000	0100	0010	= 6042
Ciphertext	6042		0110	0000	0100	0010	
Key	BEEF	\oplus	1011	1110	1110	1111	
Plaintext		=	1101	1110	1010	1101	= DEAD

Real Simple: Same key to encode and decode

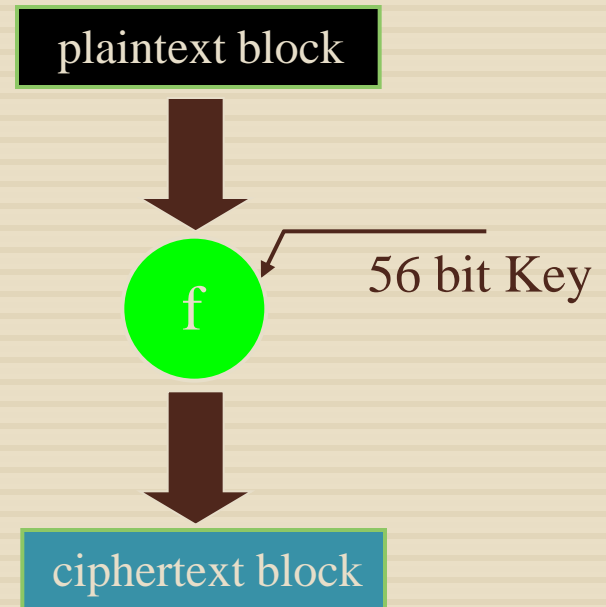
DES Advantages:

Very Fast:

Ideally suited for implementation in hardware (bit shifts, look-ups etc).

Dedicated hardware (in 1996) could run DES at 200 Mbyte/s.

Well suited for voice, video etc.



DES Security:

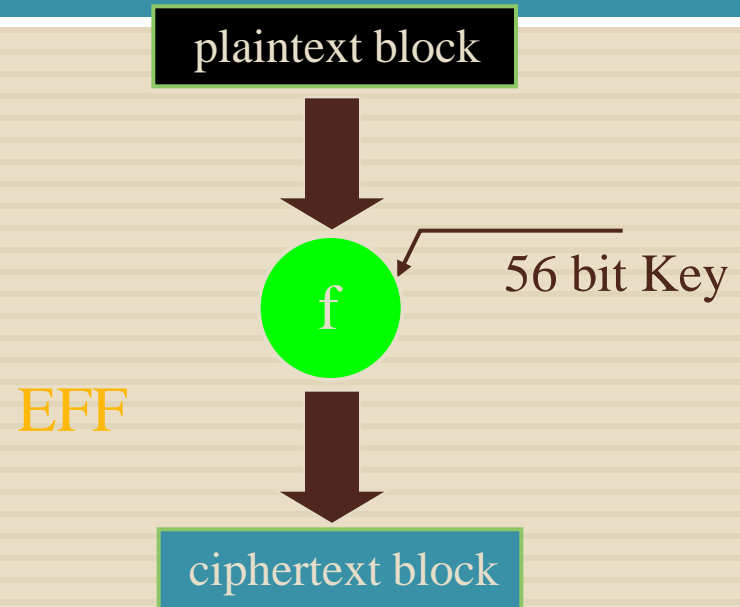
Not too good:

Trying all 2^{56} possible keys is not that hard these days.

If you spend ~\$25k you can build a DES password cracker that can will succeed in a few hours.

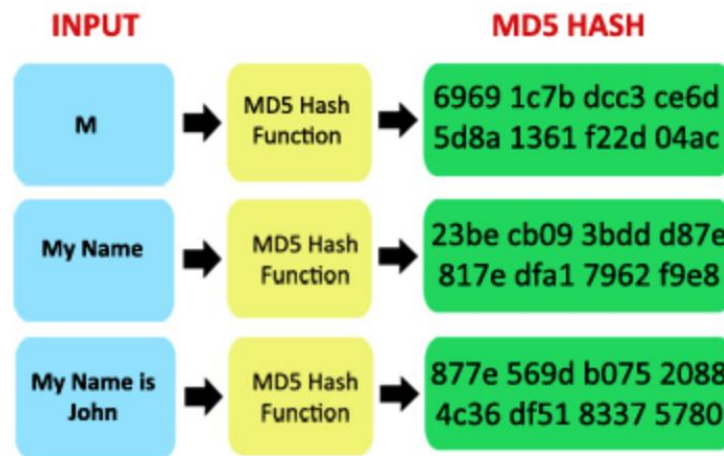
Back in 1975 this would have cost a few billion \$\$\$. It is widely believed that the NSA did this.

Similar algorithms with longer keys are available today (IDEA).



HASH

11



SHA1

- It produces a 160-bit digest from a message with a maximum length of $(2^{64} - 1)$ bits, and resembles the MD5 algorithm

SHA2

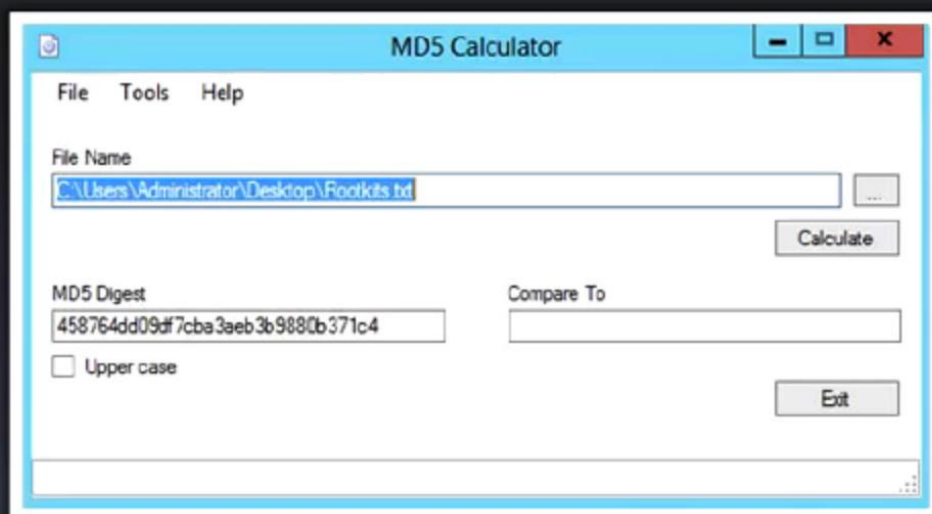
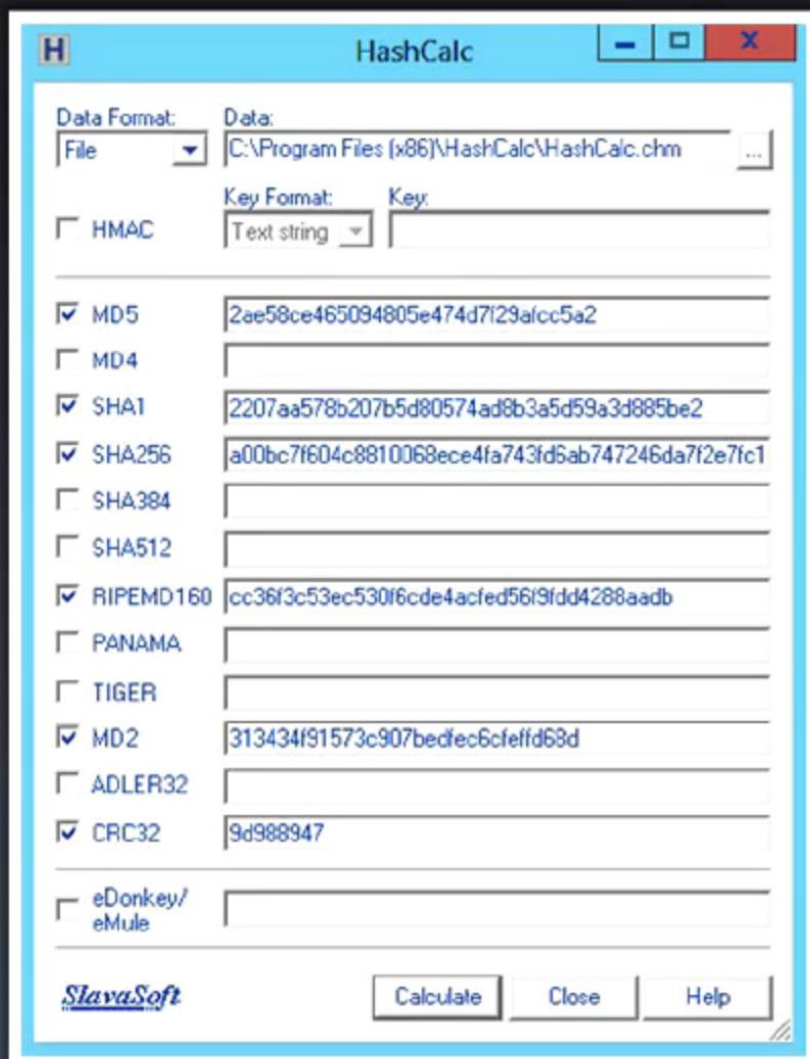
- It is a family of two similar hash functions, with different block sizes, namely SHA-256 that uses 32-bit words and SHA-512 that uses 64-bit words

SHA3

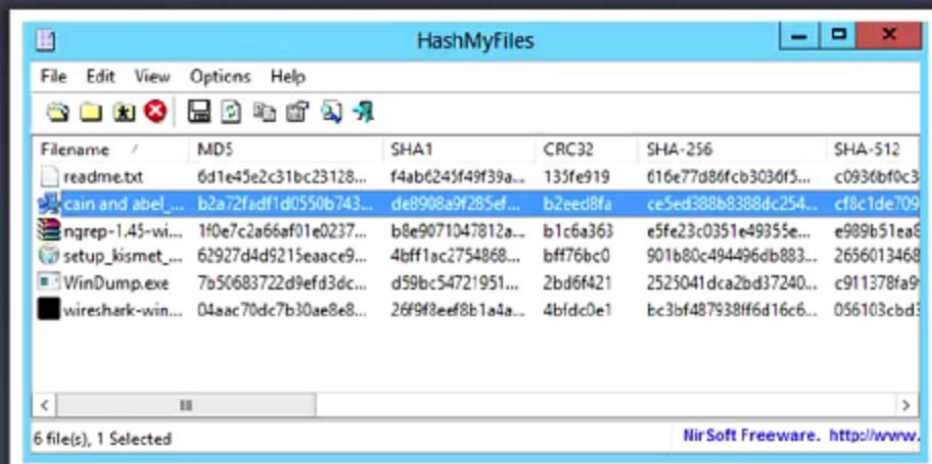
- SHA-3 uses the sponge construction in which message blocks are XORed into the initial bits of the state, which is then invertibly permuted

Hash Tool

12



<http://www.bullzip.com>



RSA (Rivest, Shamir, Adleman: 1977)

IDEA: Alice has a “public” encryption key that everyone knows, and a “private” decryption key that only she knows. Bob looks up her public key, encrypts his message, and sends it to her. She decrypts it with her private key.

- 1) Pick two large prime numbers p and q . These are secret.
- 2) Calculate $n = pq$
- 3) Pick another number e such that e and $(p-1)(q-1)$ are relatively prime.
- 4) The numbers n and e make up your public key. Publish them!
- 5) Calculate d such that $ed = 1 \bmod (p-1)(q-1)$ {i.e. $d = e^{-1} \bmod (p-1)(q-1)$ }
- 6) The number d is your private key.

Encrypt message m via $c = m^e \bmod n$

Decrypt the ciphertext c via $m = c^d \bmod n$

This is what happens when you buy a book from Amazon.com

Example:

- This is an extremely simple example and would not be secure using primes so small, normally the primes p and q would be much larger.
- Select the prime integers $p=11$, $q=3$.
- $n=pq=33$; $\phi(n)=(p-1)(q-1)=20$
- Choose $e=3$
 - Check $\gcd(3,20)=1$
- Compute $d=7$
 - $(3)d \equiv 1 \pmod{20}$
- Therefore the public key is $(n, e) = (33, 3)$ and the private key is $(n, d) = (33, 7)$.
- Now say we wanted to encrypt the message $M=7$
- $C = M^e \bmod n$
- $C = 7^3 \bmod 33$
- $C = 343 \bmod 33$
- $C = 13$

Example:

So now the cyphertext C has been found. The decryption of C is performed as follows.

$$M' = C^d \bmod n$$

$$M' = 13^7 \bmod 33$$

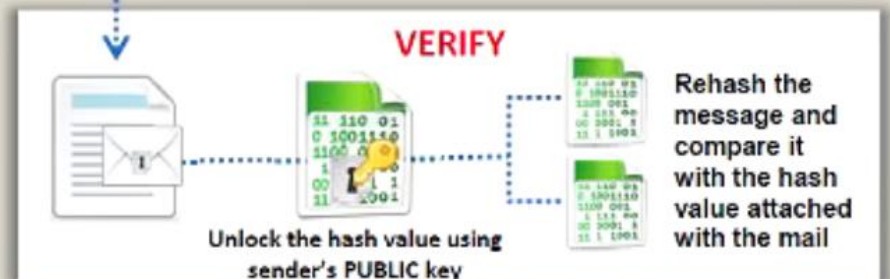
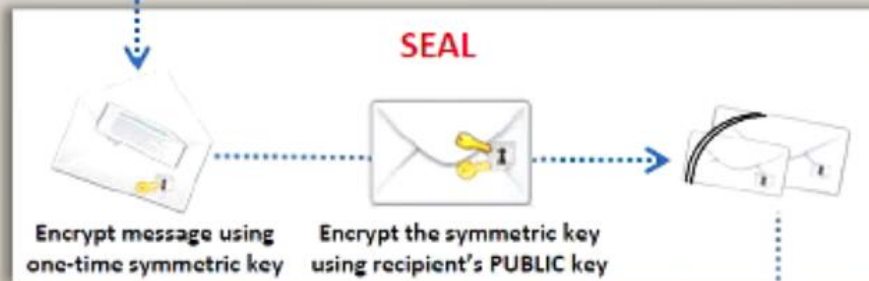
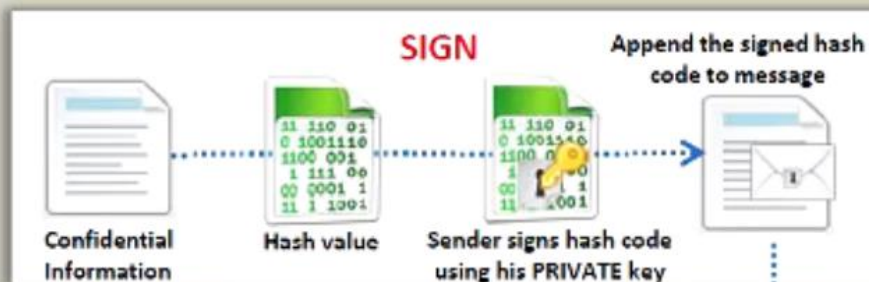
$$M' = 62,748,517 \bmod 33$$

$$M' = 7$$

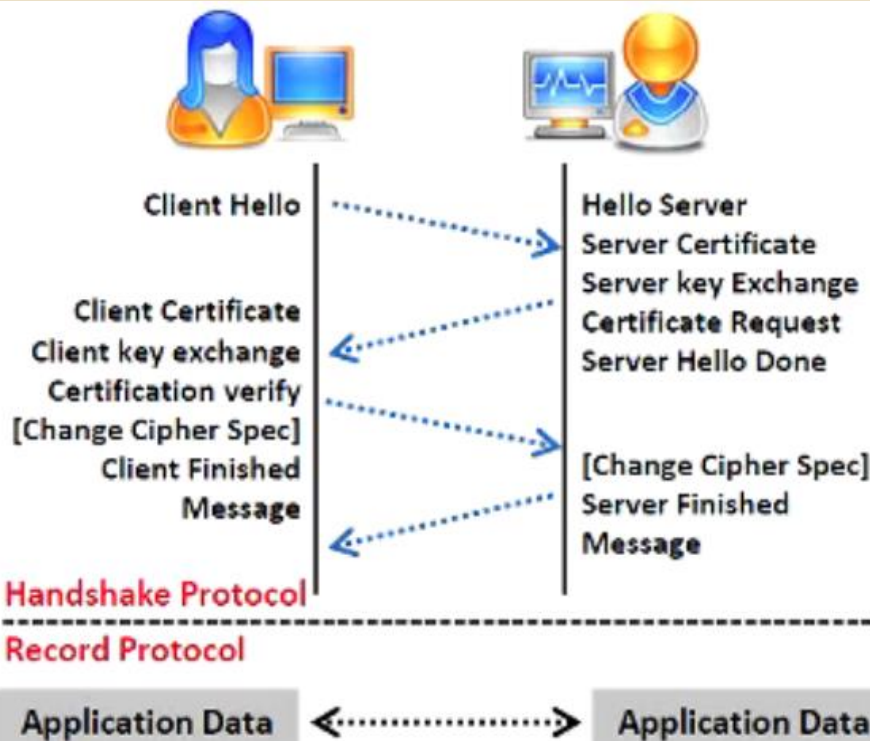
As you can see after the message has been encrypted and decrypted the final message M' is the same as the original message M. A more practical way to use the algorithm is to convert the message to hexadecimal and perform the encryption and decryption steps on each octet individually.

SSL

16



- TLS is a protocol **to establish a secure connection** between a client and a server and ensure privacy and integrity of information during transmission
- It uses the RSA algorithm with 1024 and 2048 bit strengths



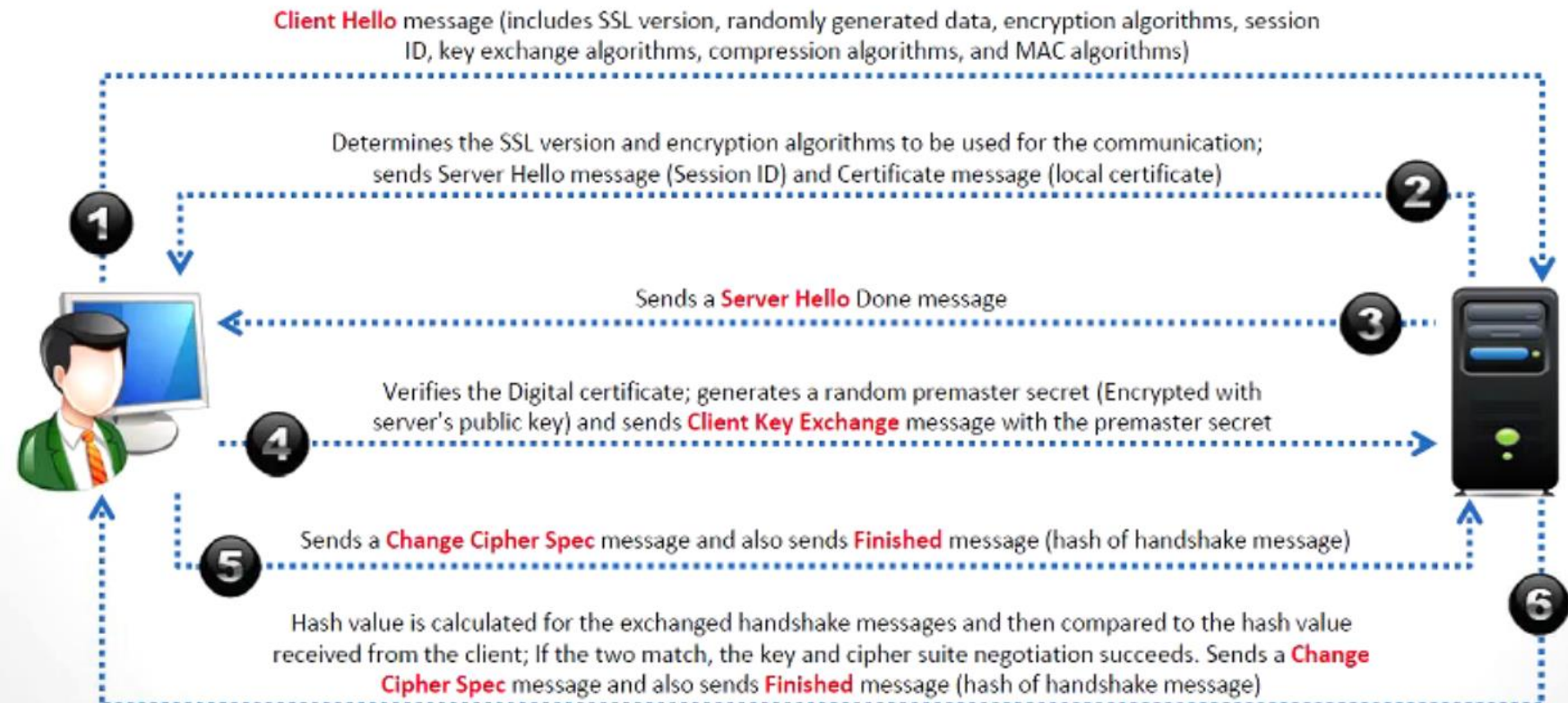
Digital Signature Algorithm

FIPS 186-2 specifies the Digital Signature Algorithm (DSA) that may be used in the generation and verification of digital signatures for sensitive, unclassified applications

RSA(SSL)

18

- It uses **RSA asymmetric (public key) encryption** to encrypt data transferred over SSL connections



Attacks

19



Trickery and Deceit

It involves the use of social engineering techniques to extract cryptography keys



Brute-Force

Cryptography keys are discovered by trying every possible combination



One-Time Pad

A one-time pad contains many non-repeating groups of letters or number keys, which are chosen randomly



Frequency Analysis

It is the study of the frequency of letters or groups of letters in a ciphertext

It works on the fact that, in any given stretch of written language, certain letters and combinations of letters occur

Brute-Force

20

Attack Scheme

Defeating a cryptographic scheme by **trying a large number of possible keys** until the correct encryption key is discovered



Brute-Force Attack

Brute-force attack is a **high resource and time intensive process**, however, more certain to achieve results



Success Factors

Success of brute force attack depends on **length of the key, time constraint, and system security mechanisms**



Power/Cost	40 bits (5 char)	56 bit (7 char)	64 bit (8 char)	128 bit (16 char)
\$ 2K (1 PC. Can be achieved by an individual)	1.4 min	73 days	50 years	10^{20} years
\$ 100K (this can be achieved by a company)	2 sec	35 hours	1 year	10^{19} years
\$ 1M (Achieved by a huge organization or a state)	0.2 sec	3.5 hours	37 days	10^{18} years

RSA Security:

RSA is secure because its very hard to factor n to find p and q if n is sufficiently big. (Discrete logarithms).

“Sufficiently Big” means ~ 2048 bits

“Hard” means that all the computers on earth could not do it in the age of the universe.

TrueCrypt

- TrueCrypt is disk encryption software that **creates a virtual encrypted disk** within a file and mounts it as a real disk
- It encrypts an **entire partition or storage device** such as USB flash drive or hard drive



<http://www.truecrypt.org>



Certification

23

COMODO
Creating Trust Online®

SEARCH OUR WEBSITE GO

Products | Home & Home Office | E-Commerce | Small to Medium Business | Large Enterprise | Partners | Social Media

The First To Bring You a Full Line of 2048-bit Certificates

Comodo brings you next generation compliance today with our line of 2048-bit SSL.

Explore Our SSL Certificates

- Secure Subdomains
- Secure a Website
- Secure a Mail Server
- Secure a Web Server
- Secure a Mail Server

[SHOP CERTIFICATES](#)

FREE PRODUCTS | HOME COMPUTING | BUSINESS SOLUTIONS | E-COMMERCE SOLUTIONS | ENTERPRISE SOLUTIONS

<http://www.comodo.com>

thawte

Products | Partners | Support | Resources | My Account

online security trusted by millions around the world

Get started with SSL
Discover what SSL is and why you need it. [Learn more](#)

Inspire Trust Online
Show Users the Thawte Trusted Site Seal and Green Bar. [Learn now](#)

Simplify SSL Security
Just one SAN certificate can secure multiple domains. [Learn how](#)

BUY CERTIFICATES

BUY SSL Certificates

BUY Code Signing Certificates

the most visible web site security

<https://www.greenSSL.com> Identified by Thawte

<http://www.thawte.com>

Symantec VeriSign Authentication Services

Products & Services | Partners | Support | My Account

Same check. New name. Still the gold standard.

The same security, services and support you've come to trust from VeriSign are now brought to you by Symantec.

What it means for you >

Trust from Search to Browse to Buy

Boost your site traffic and conversions with powerful trust features. Free with every SSL Certificate.

Protect Your Site. Grow Your Business.

New features from Symantec SSL make your Web site **easy to trust and easy to secure**

VERISIGN

Cyber security and availability products your business relies on:

- Managed DNS
- ULAS PROTECTION
- iDefense™
- Domain Name Services

are available from Verisign at VerisignInc.com

Entrust

SECURITY ON: SSL
Certificate Management Services

Leverage a centralized certificate management hub to simplify the purchase, deployment, renewal and expiry of all digital certificates

> Why Entrust | > Products | > Support | > Partners | > About Us | > My Account

Go Wild!
New Wildcard SSL Certificates
From **\$725/year** [Buy Now](#) [Learn More](#)

EV Multi-Domain SSL Certificates
From **\$373/year** [Buy Now](#) [Learn More](#)

UC Multi-Domain SSL Certificates
From **\$249/year** [Buy Now](#) [Learn More](#)

Advantage SSL Certificates
From **\$186/year** [Buy Now](#) [Learn More](#)

Standards SSL Certificates
From **\$155/year** [Buy Now](#) [Learn More](#)

Personal Secure Email
Enterprise Secure Email
Code Signing Certificates
Adobe ACS Signed Certificates
Certificate Management Service
Certificate Recovery