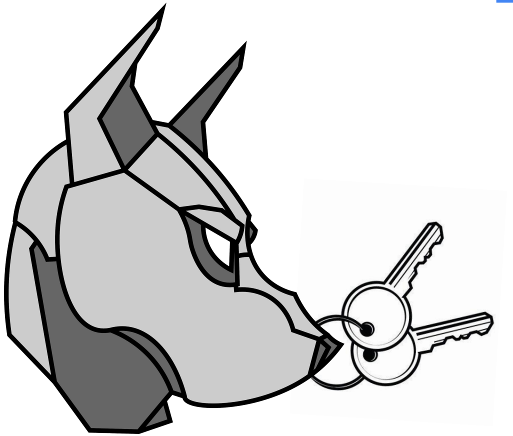
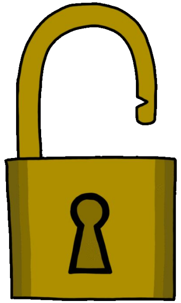
Cyber Defense Organization

Fall 2020 - Encryption/Cryptography





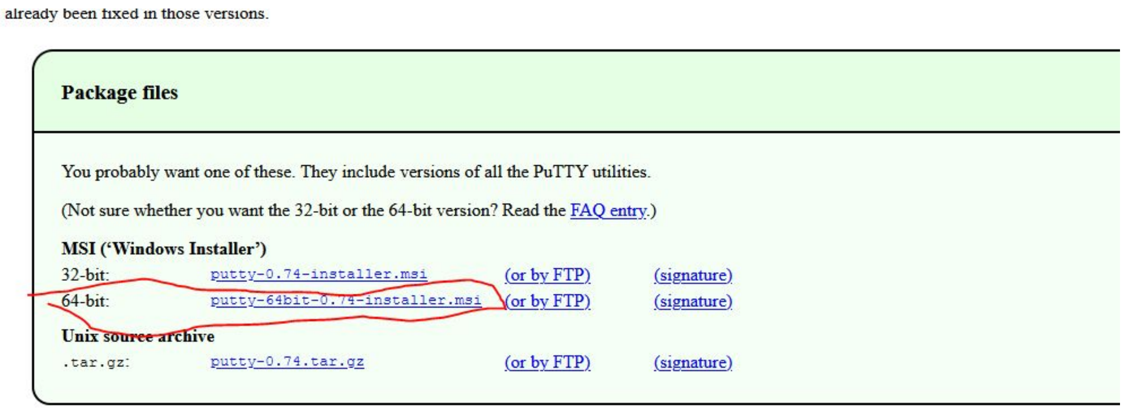
Attendance

https://forms.gle/hrQfSqmqHPMkAD2S7

Word of the week:

Downloading putty

- Let’s do this now so we are ready for the hands on section!!!
- https://www.putty.org/



already been fixed in those versions.

Package files

You probably want one of these. They include versions of all the PuTTY utilities.

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

MSI (‘Windows Installer’)

32-bit:	putty-0.74-installer.msi	(or by FTP)	(signature)
64-bit:	putty-64bit-0.74-installer.msi	(or by FTP)	(signature)

Unix source archive

.tar.gz:	putty-0.74.tar.gz	(or by FTP)	(signature)

Silly Putty
4+
The Original
⚠ WARNING: CHOKING HAZARD - Small parts. Not for children under 3 yrs.
⚠ AVERTISSEMENT : RISQUE DE SUFFOCATION - Petites pièces. Ne convient pas aux enfants de moins de 3 ans.
Silly Putty

What is encryption??

The process of converting information or data into a code, especially to prevent unauthorized access

The word “cryptography” technically means the art of writing codes.

Why should you care? Capture the flags love some Crypto questions.

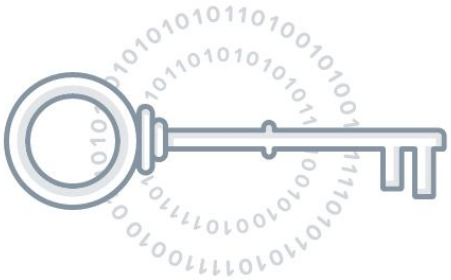
=P

Encryption vs Encoding vs Hashing

	Encryption	Encoding	Hashing
Goal	Maintaining data confidentiality	Ease of use/compression.	Ensure integrity of data, used in forensics
Key used?	Yes	No	No
Reversible?	Yes	Yes	No

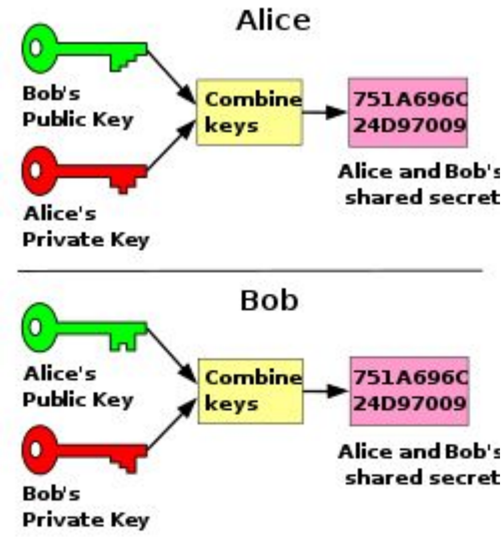
Keys

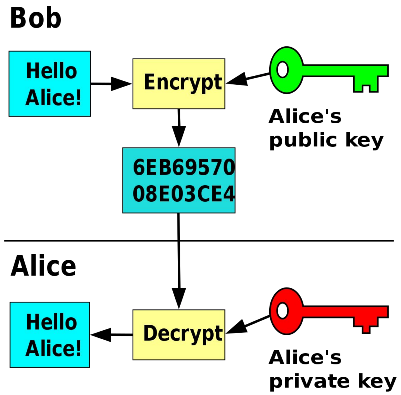
An encryption key is a random string of bits created explicitly for scrambling and unscrambling data. Encryption keys are designed with algorithms intended to ensure that every key is unpredictable and unique.



Public key encryption

- Also known as asymmetric encryption
- Form of encryption where keys come in pairs. What one key encrypts, only the other can decrypt.
- One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

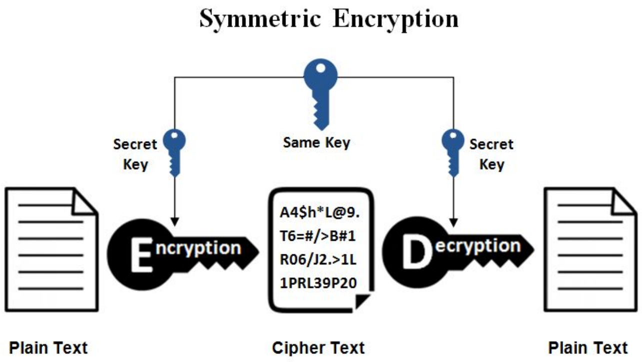




Private key encryption

Symmetric key encryption.

- a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.



Advantages & Disadvantages

Asymmetric Encryption

Advantages:

- More secure than symmetric (uses two keys instead of one)
- Secure key distribution is not an issue

Disadvantages:

- Too slow (takes a lot of resources to do)
- Requires a lot of keys (two keys per person)

Symmetric Encryption

Advantages:

- Faster than asymmetric encryption
- Less keys needed

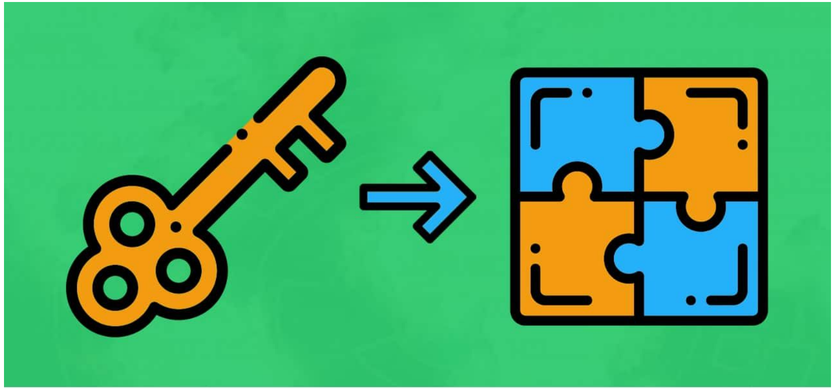
Disadvantages:

- Secure key distribution is an issue
- Less secure (if the key is exposed your done)

Hashing

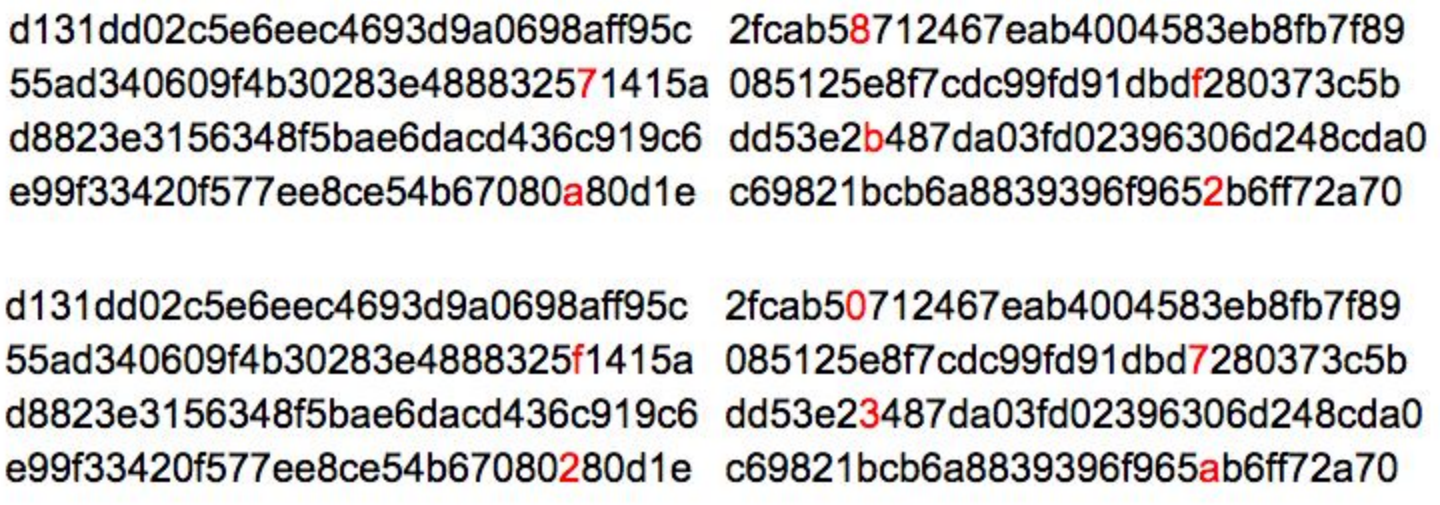
Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms.

One way algorithm. TL;DR You can turn a chicken into a nugget… but its very hard to turn a chicken nugget back.



What is Hashing?

Hashing Collisions



```
d131dd02c5e6eec4693d9a0698aff95c 2fcab58712467eab4004583eb8fb7f89
55ad340609f4b30283e488832571415a 085125e8f7cdc99fd91dbdf280373c5b
d8823e3156348f5bae6dacd436c919c6 dd53e2b487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080a80d1e c69821bcb6a8839396f9652b6ff72a70

d131dd02c5e6eec4693d9a0698aff95c 2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325f1415a 085125e8f7cdc99fd91dbd7280373c5b
d8823e3156348f5bae6dacd436c919c6 dd53e23487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080280d1e c69821bcb6a8839396f965ab6ff72a70
```

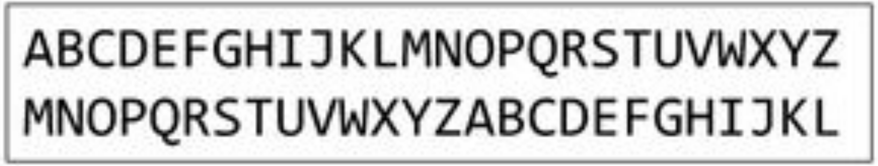
Each of these blocks has MD5 hash 79054025255fb1a26e4bc422aef54eb4.

https://www.links.org/?p=6

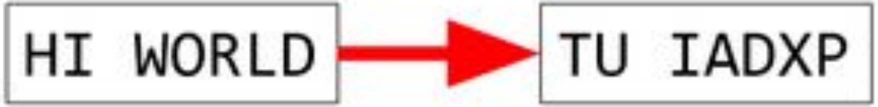
Caeser Cipher/ROT13

The Caesar Cipher or Caesar Shift is a cipher which uses the alphabet in order to encode texts.

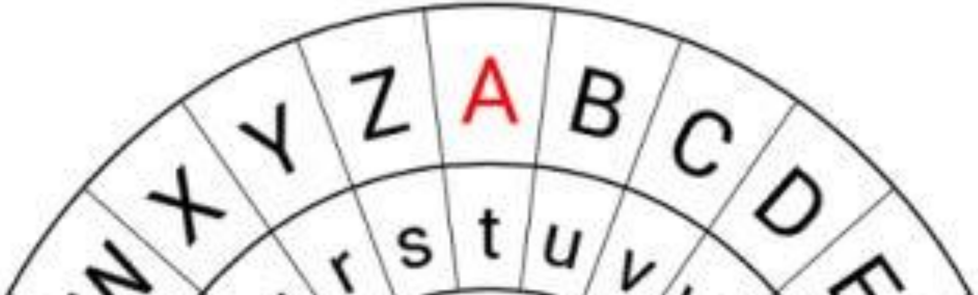
The Caesar Cipher or Caesar Shift is a cipher which uses the alphabet in order to encode texts.



ABCDEFGHIJKLMNOPQRSTUVWXYZ
MNOPQRSTUVWXYZABCDEFGHIJKL



HI WORLD → TU IADXP



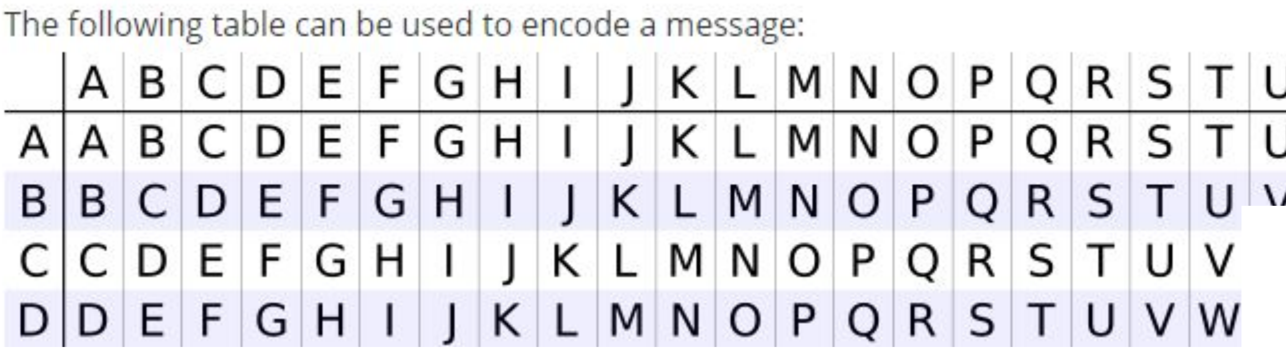
Vigenere Cipher

A Vigenere Cipher is an extended Caesar Cipher where a message is encrypted using various Caesar shifted alphabets.

Plaintext: ATTACKATDAWN

Key: LEMONLEMONLE

Ciphertext: LXFOPVEFRNHR



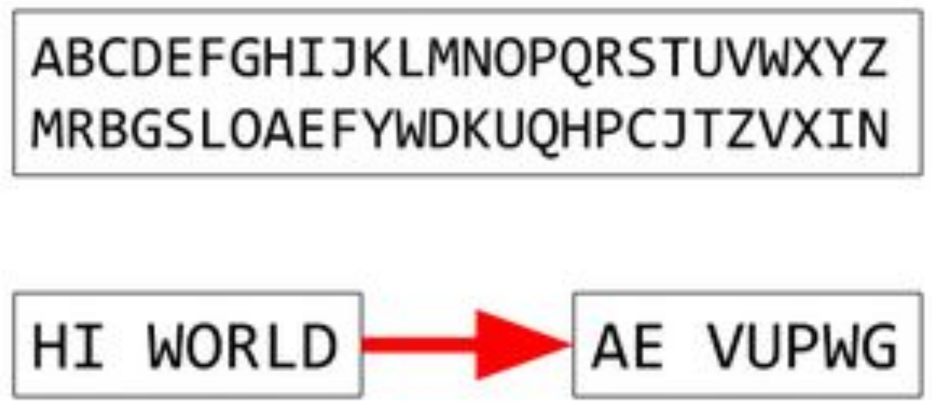
The following table can be used to encode a message:

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

Substitution

A Substitution Cipher is system of encryption where different symbols substitute a normal alphabet.

To identify - Look for spaces, punctuation, and general word/sentence structure. Vulnerable to most frequency analysis attacks.



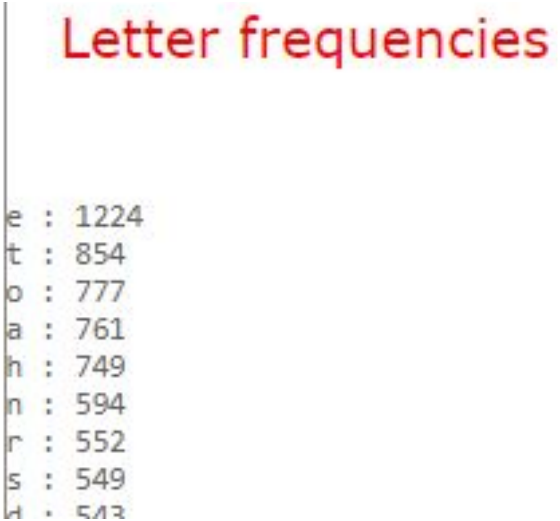
ABCDEFGHIJKLMNOPQRSTUVWXYZ
MRBGSLOAEFYWDKUQHPCJTZVXIN

HI WORLD → AE VUPWG

Anti-Encryption: Frequency Analysis

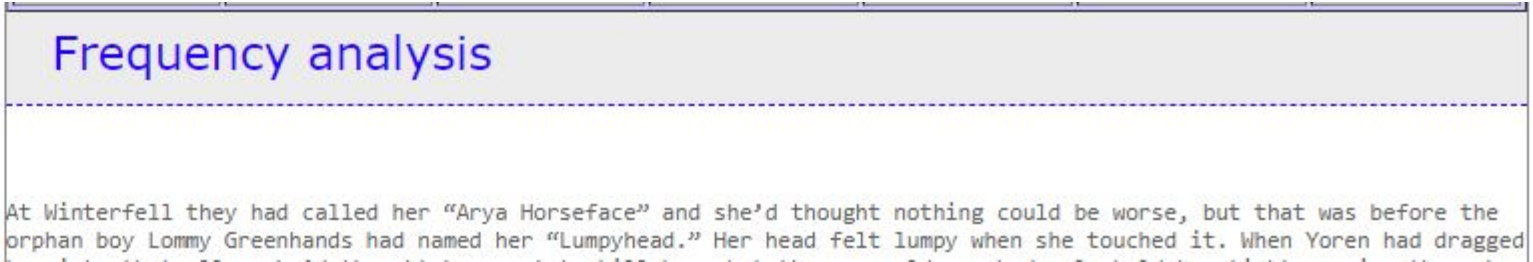
Encrypted text is sometimes achieved by replacing one letter by another. To start deciphering the encryption it is useful to get a frequency count of all the letters.

http://www.richkni.co.uk/php/crypta/freq.php



Letter frequencies

```
e : 1224
t : 854
o : 777
a : 761
h : 749
n : 594
r : 552
s : 549
d : 543
```



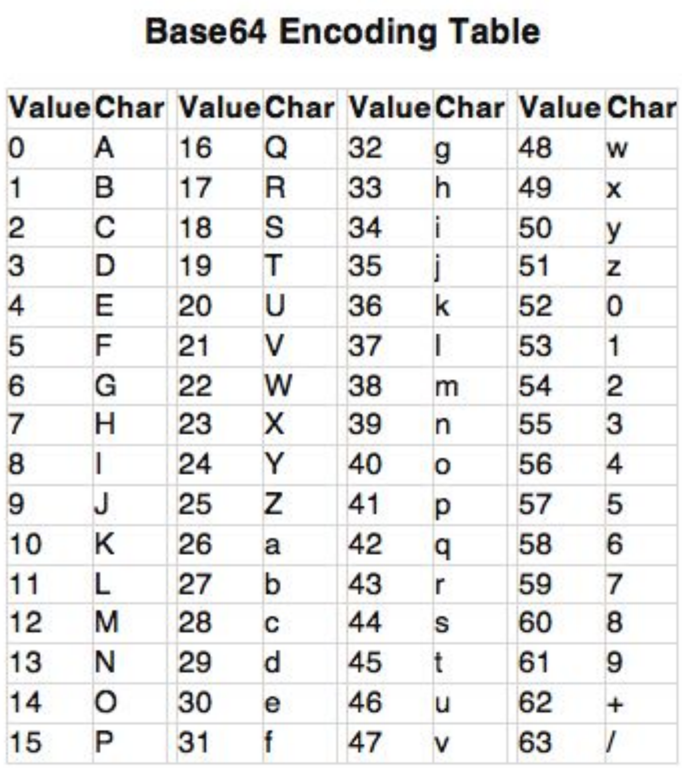
Frequency analysis

```
At Winterfell they had called her “Arya Horseface” and she’d thought nothing could be worse, but that was before the
orphan boy Lommy Greenhands had named her “Lumpyhead.” Her head felt lumpy when she touched it. When Yoren had dragged
```

Base64

Base64 is a mechanism to enable representing and transferring binary data over mediums that allow only printable characters. It is the most popular form of the “Base Encoding”, the others known in use being Base16 and Base32.

How to recognize it: usually base64 includes a == at the end of the encoding

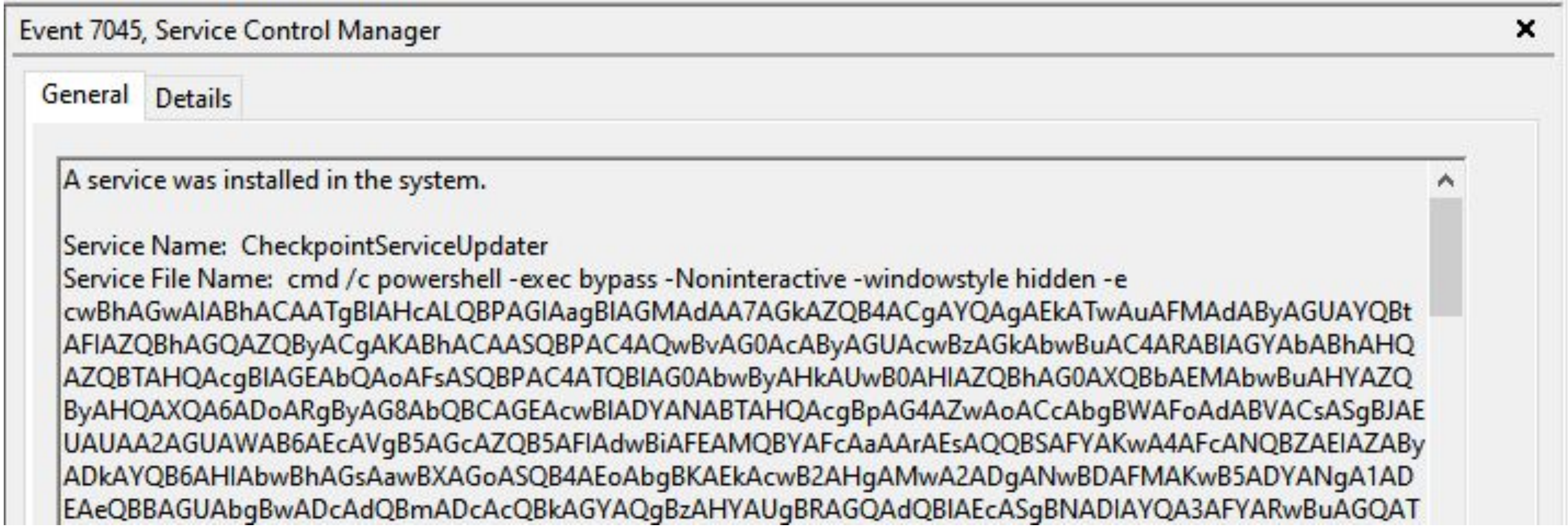


Base64 Encoding Table

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Base64 in real world

Base64 is used in the “Real world” a lot for commands. It is a cheap and easy way to remove spaces and punctuation. If you see this... its probably bad.



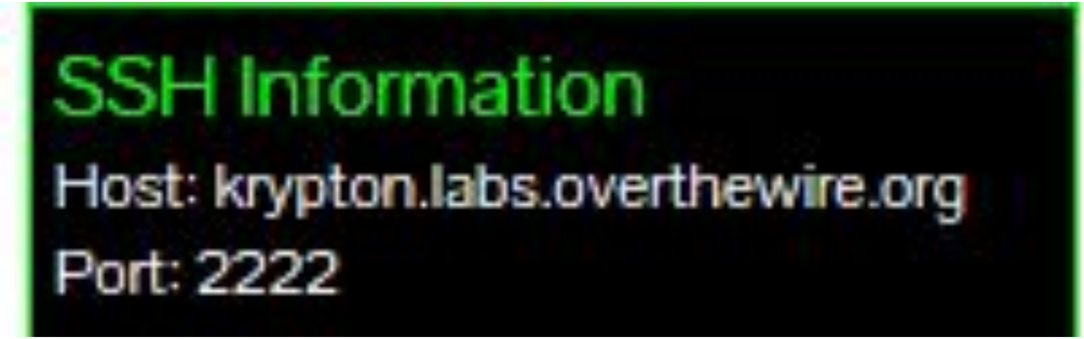
```
A service was installed in the system.

Service Name:  CheckpointServiceUpdater
Service File Name:  cmd /c powershell -exec bypass -Noninteractive -windowstyle hidden -e
```

```
cwBhAGwAIABhACAATgBIAHcALQBPAGIAagBIAGMAdAA7AGkAZQB4ACgAYQAgAEkATwAuAFMAdAByAGUAYQBt
AFIAZQBhAGQAZQByACgAKABhACAASQBPAC4AQwBvAG0AcAByAGUAcwBzAGkAbwBuAC4ARABIAGYAbABhAHQ
AZQBTAHQAcgBIAGEAbQAoAFsASQBPAC4ATQBIAG0AbwByAHkAUwB0AHIAZQBhAG0AXQBbAEMAbwBuAHYAZQ
ByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBIADYANABTAHQAcgBpAG4AZwAoACcAbgBWAFoAdABVACsASgBJAE
UAUAA2AGUAWAB6AEcAVgB5AGcAZQB5AFIAdwBiAFEAMQBYAFcAaAArAEsAQQBSAFYAKwA4AFcANQBZAEIAZABy
ADkAYQB6AHIAbwBhAGsAawBXAGoASQB4AEoAbgBKAEkAcwB2AHgAMwA2ADgANwBDAFMAKwB5ADYANgA1AD
EAeQBBAGUAbgBwADcAdQBmADcAcQBkAGYAQgBzAHYAUgBRAGQAdQBIAEcASgBNADIAYQA3AFYARwBuAGQAT
```

Activity Time!

https://overthewire.org/wargames/krypton/krypton0.html



SSH Information

Host: krypton.labs.overthewire.org

Port: 2222

Coming up next week!

Tuesday: Blue Team Practice @ 7pm

Wednesday: Security + @ 5pm

Thursday: Red Team Practice @ 7:30pm

Friday: Forensics something @ 3:30pm

Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!