Applied cryptography

Code Breaker

- Given the ciphertext of Caesar cipher, try to find the plaintext (without using automated solutions) using the tool http://inventwithpython.com/cipherwheel/

1. LQIRUPDWLRQ VHFXULWB LV WKH EHVW
2. RIXASVOW MW FSVMRK

What are the plaintext? menti

Brute Force attack

1. Brute Force attack

Example 1: LQIRUPDWLRQ VHFXULWB LV WKH EHVW

- Write Caesar decryption with Cryptool2
- Brute Force attack: trying every possible key one by one and checking whether the resulting plaintext is meaningful.

Heuristics

2. Heuristics based on the language

Example 2: EPG QA XTGUWCBP ITEIGA EMB?

Frequency analysis

3. Frequency analysis: the letters of the ciphertext are the same as those of the plaintext, a frequency analysis on the ciphertext would reveal that each letter has approximately the same likelihood as in English.

Example 3: given English ciphertext as in the next slide

Frequency test with Cryptool2

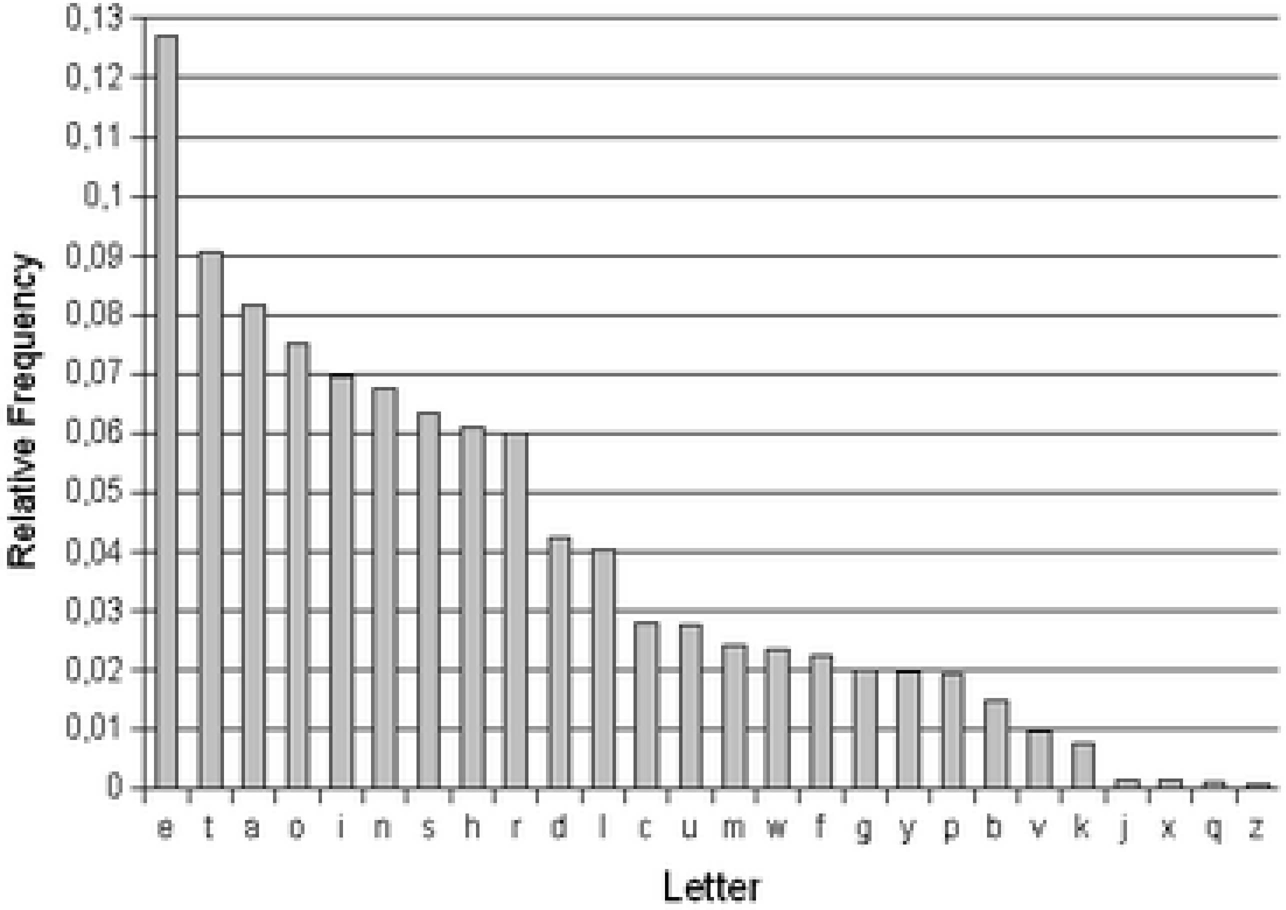
NZYQFDPO LMZFE ESP CFWPD? JZF’CP YZE ESP ZYWJ ZYP
“ESPCP’D L WZE ZQ CPNJNWTYR XJESD ZFE ESPCP, LYO NZYQFDTZY, LYO ESLE’D WLCRPWJ OZHY EZ L WLNV ZQ NZYDTDEPYNJ MPEHPPY NZFYNTWD,” DLJD ULXPD. “ZQEPY APZAWP HTWW OZ ESP HCZYR ESTYR LYO YZE CPLWWJ FYOPCDELYO HSLE’D CTRSE ZC HCZYR.”

HP’CP YZE GPCJ RZZO LE VPPATYR ESTYRD DTXAWP LYO PIAWLTYTYR ESP ACTYNTAWPD...
SLGTYR MPPY TY ESP TYOFDECJ QZC ZGPC L OPNLOP, LYO DAPYE L WZE ZQ ETXP HZCVTYR HTES CPNJNWTYR ACZQPDDTZYLWD, ULXPD CPLWTDPO SP SLO LY ZAAZCEFYTEJ EZ HCTEP OZHY LWW ESP CFWPD LYO ACTYNTAWPD ESLE SP’O RLESPCPO ZGPC ESP JPLCD. SP HPYE ESCZFRS GLCTZFD HPMDTEPD WTVP CPNJNWPYZH.NZX, CFY MJ ESP NSLCTEJ HCLA (ESP HLDEP LYO CPDZFCNPD LNETZY ACZRCLXXP), TYEPCGTPHPO NZWWPLRFPD TY ESP TYOFDECJ LYO CPNJNWPCD ESPXDPWGPD LYO LDVPO – HSLE XLVPD DZXPESTYR XZCP WTVPWJ EZ XLVP TE ESCZFRS ESP ACZNPDD LYO MP CPNJNWPO?

“ZYP ESTYR T’GP YZETNPO TD HP’CP YZE GPCJ RZZO LE VPPATYR ESTYRD DTXAWP LYO PIAWLTYTYR ESP ACTYNTAWPD,” DLJD ULXPD. “HSPY T HLD DPEETYR ZFE EZ HCTEP L MZZV, T HLYEPO EZ OTDETW TE OZHY TYEZ CPLWWJ DTXAWP TYQZCXLETZY ESLE APZAWP NZFWO CPXPXMPC.”

SPCP LCP DZXP ZQ ULXPD’D EZA ETAD QZC RPEETYR CPNJNWTYR CTRSE.

English frequency



Source: Wikipedia

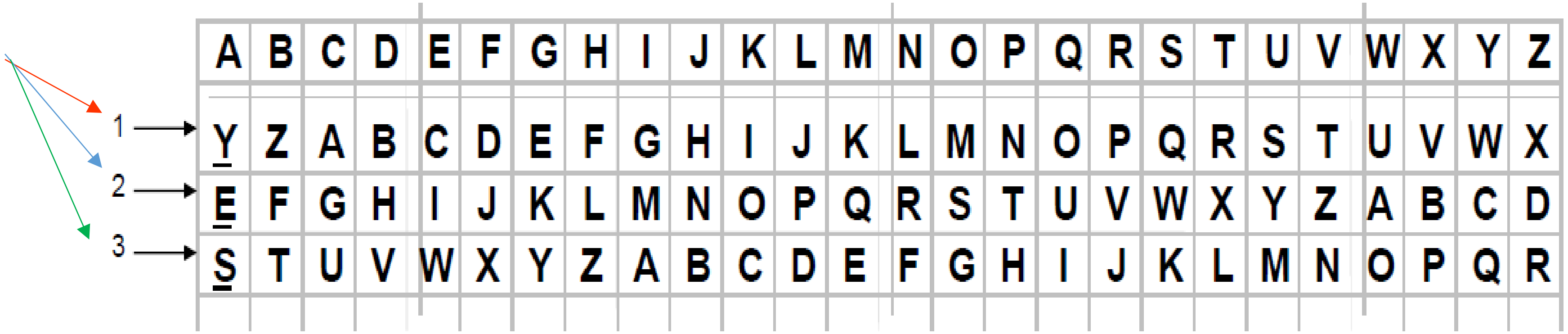
Ciphertext frequency

- ?

Make it harder – Polyalphabetic cipher

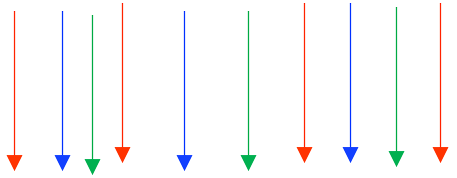
Vigenere cipher

3 substitutions



	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	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
2	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
3	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

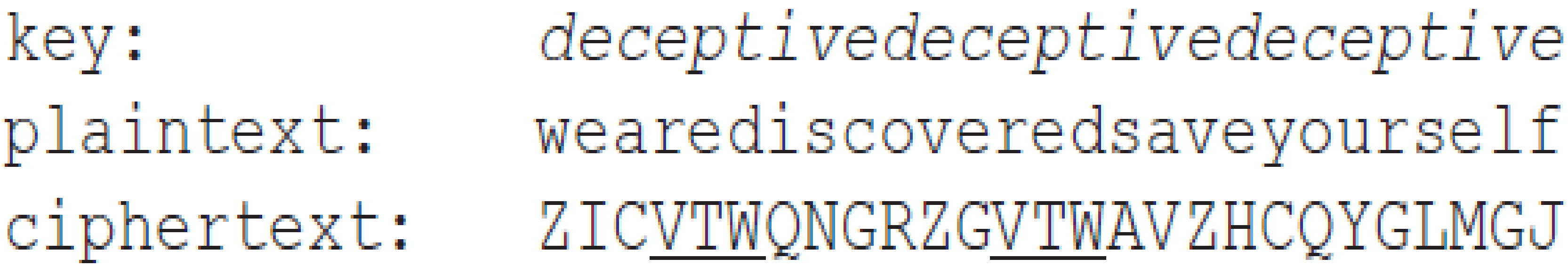
HELLO WORLD



F IDJ S ?????

menti

Cryptanalysis of Vigenere cipher

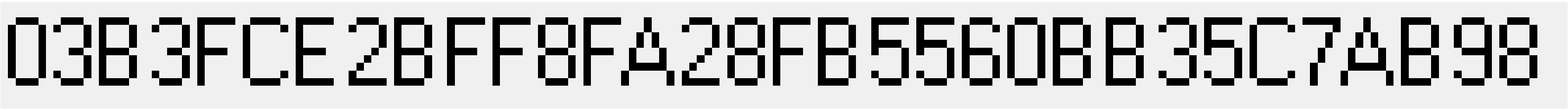


```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

- Find the key length (the number of substitutions) : ‘VTW’ repeats after 9 characters => key length is a divisor of 9 which is 3 or 9
- Frequency analysis attacks:
  - If key length = 3, run frequency analysis over 3 monoalphabetic substitutions
  - If key length = 9, run frequency analysis over 9 monoalphabetic subsitutions

Password hacking

- Given MD5 hash code of a password:



03B3FCE2BFF8FA28FB5560BB35C7AB98

What is the password?

Brute force attack

1. Brute Force: trying every possible password one by one and calculating MD5, checking whether the output is the same as the given hash code
   - Try with Cryptool2
   - Try with Cain and Abel (a **password** recovery tool for Microsoft Operating Systems)

Dictionary attack

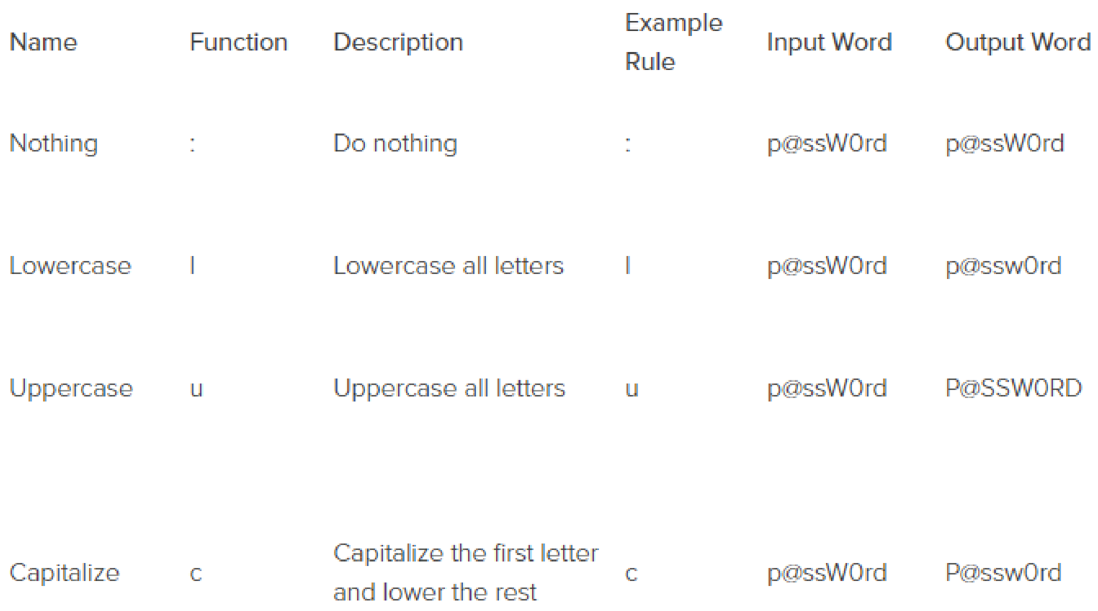
2. Dictionary:
   - Demo with Cain and Abel

Dictionary attack

2. Dictionary and rule-based

Basic dictionary list
password
mysecret
Qwerty

Want to try the above passwords with capitalized letters
PASSWORD
MYSECRET
QWERTY



Name	Function	Description	Example Rule	Input Word	Output Word
Nothing	:	Do nothing	:	p@ssW0rd	p@ssW0rd
Lowercase	l	Lowercase all letters	l	p@ssW0rd	p@ssw0rd
Uppercase	u	Uppercase all letters	u	p@ssW0rd	P@SSW0RD
Capitalize	c	Capitalize the first letter and lower the rest	c	p@ssW0rd	P@ssw0rd

https://www.4armed.com/blog/hashcat-rule-based-attack/

Hash tables

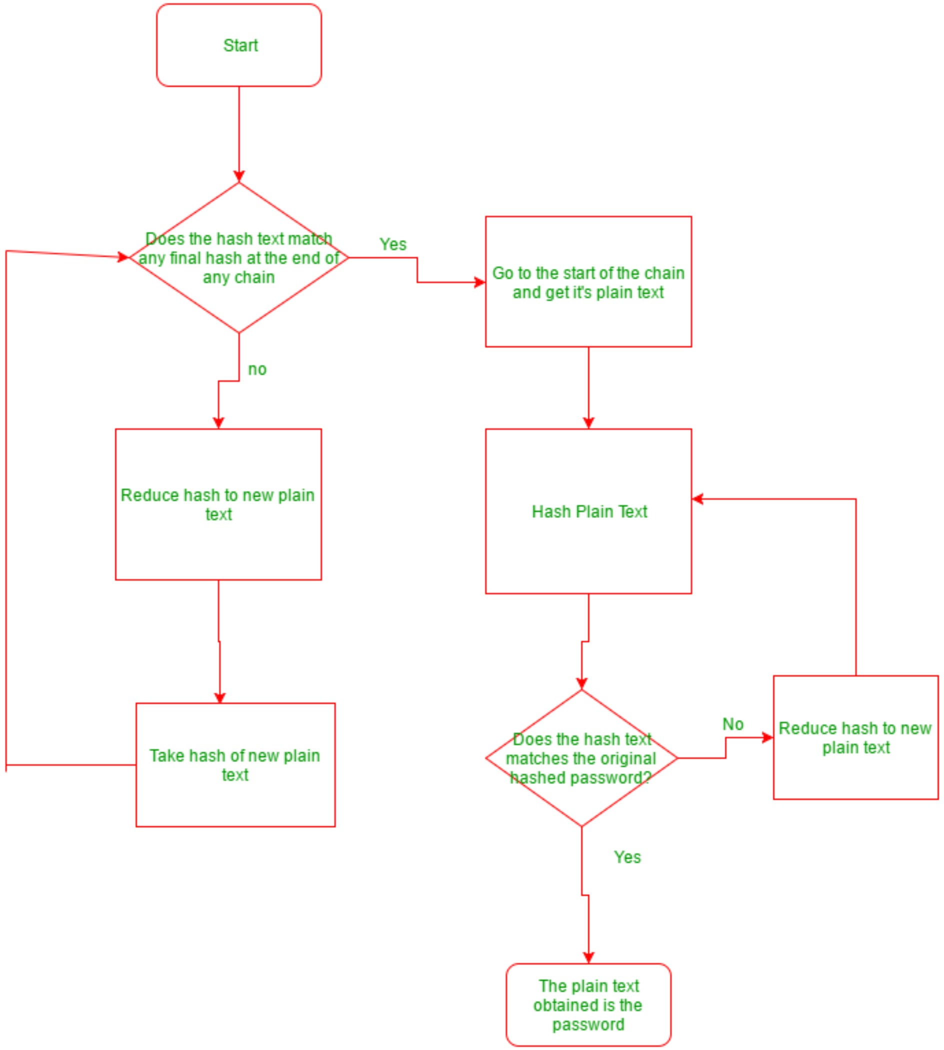
farm1990M0Of1nd1ngn3m	07dbb6e6832da0841dd79701200e4b179f1a94a7b3dd26f612817f3c03117434
farm1990M0Of1nd1ngd0ry	11c150eb6c1b776f390be60a0a5933a2a2f8c0a0ce766ed92fea5bfd9313c8f6

Hash tables and Rainbow tables

3. Rainbow tables

$$\texttt{aaaaaa} \xrightarrow[H]{} \texttt{281DAF40} \xrightarrow[R]{} \texttt{sgfnyd} \xrightarrow[H]{} \texttt{920ECF10} \xrightarrow[R]{} \texttt{kiebgt}$$

Hash Reduce



Start

Does the hash text match any final hash at the end of any chain

Yes

Go to the start of the chain and get it's plain text

no

Reduce hash to new plain text

Take hash of new plain text

Hash Plain Text

Does the hash text matches the original hashed password?

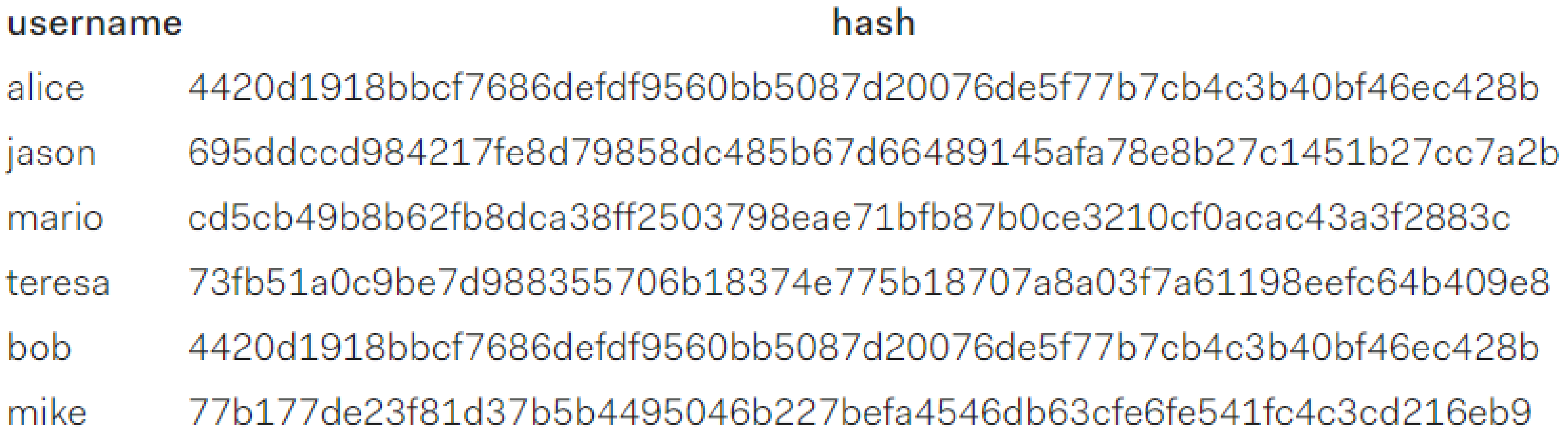
No

Reduce hash to new plain text

Yes

The plain text obtained is the password

Unsalted password



username	hash
alice	4420d1918bbcf7686defdf9560bb5087d20076de5f77b7cb4c3b40bf46ec428b
jason	695ddccd984217fe8d79858dc485b67d66489145afa78e8b27c1451b27cc7a2b
mario	cd5cb49b8b62fb8dca38ff2503798eae71bfb87b0ce3210cf0acac43a3f2883c
teresa	73fb51a0c9be7d988355706b18374e775b18707a8a03f7a61198eefc64b409e8
bob	4420d1918bbcf7686defdf9560bb5087d20076de5f77b7cb4c3b40bf46ec428b
mike	77b177de23f81d37b5b4495046b227befa4546db63cfe6fe541fc4c3cd216eb9

- What can you learn from the above table?

Salting

User: Alice

Password: farm1990M0O

Salt: f1nd1ngn3m0

Salted input:
farm1990M0Of1nd1ngn3m0

Hash (SHA-256):
07dbb6e6832da0841dd7970
1200e4b179f1a94a7b3dd26f
612817f3c03117434

User: Bob

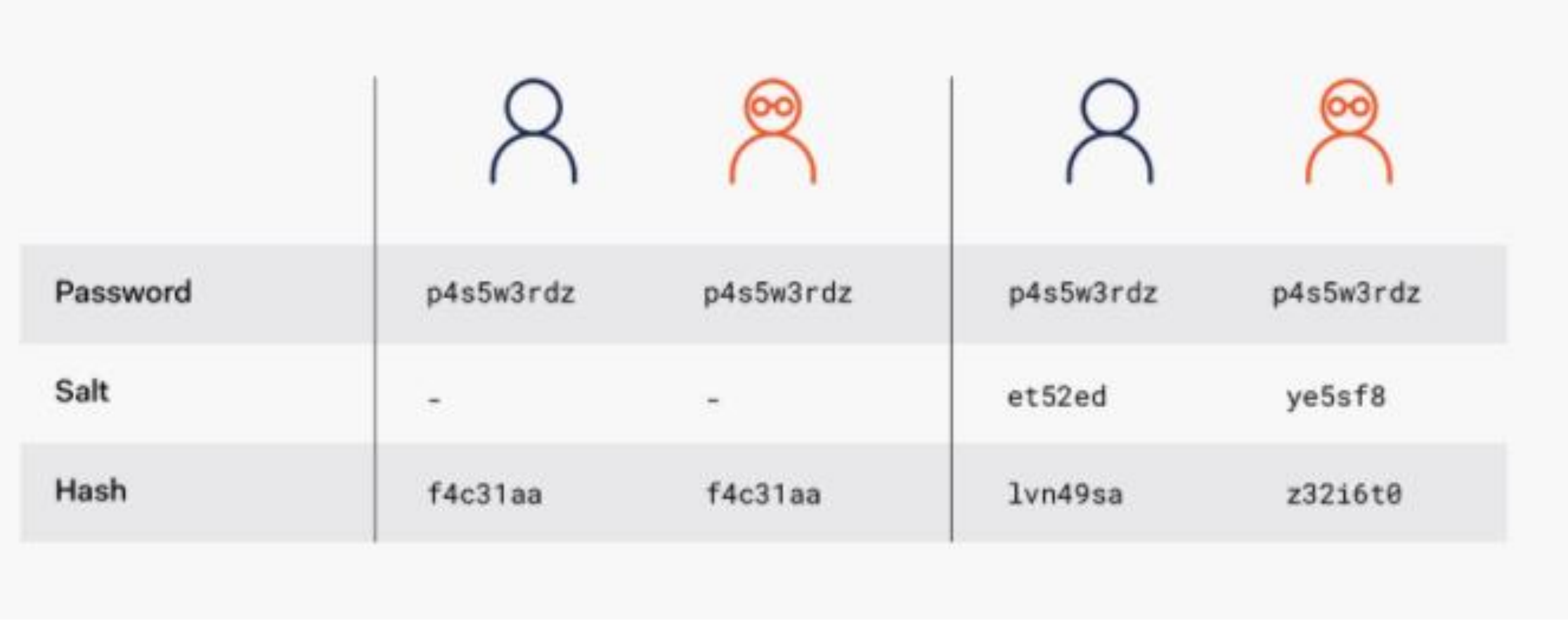
Password: farm1990M0O

Salt: f1nd1ngd0ry

Salted input:
farm1990M0Of1nd1ngd0ry

Hash (SHA-256):
11c150eb6c1b776f390be60a
0a5933a2a2f8c0a0ce766ed9
2fea5bfd9313c8f6

Unsalted vs Salted



Password	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz
Salt	-	-	et52ed	ye5sf8
Hash	f4c31aa	f4c31aa	lvn49sa	z32i6t0

Devising your own secure communications

- Group, menti

The origins of Public Key Cryptography

- Watch together