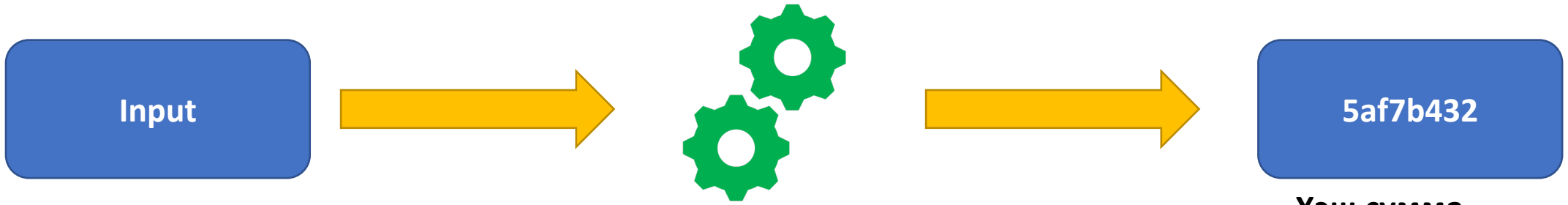
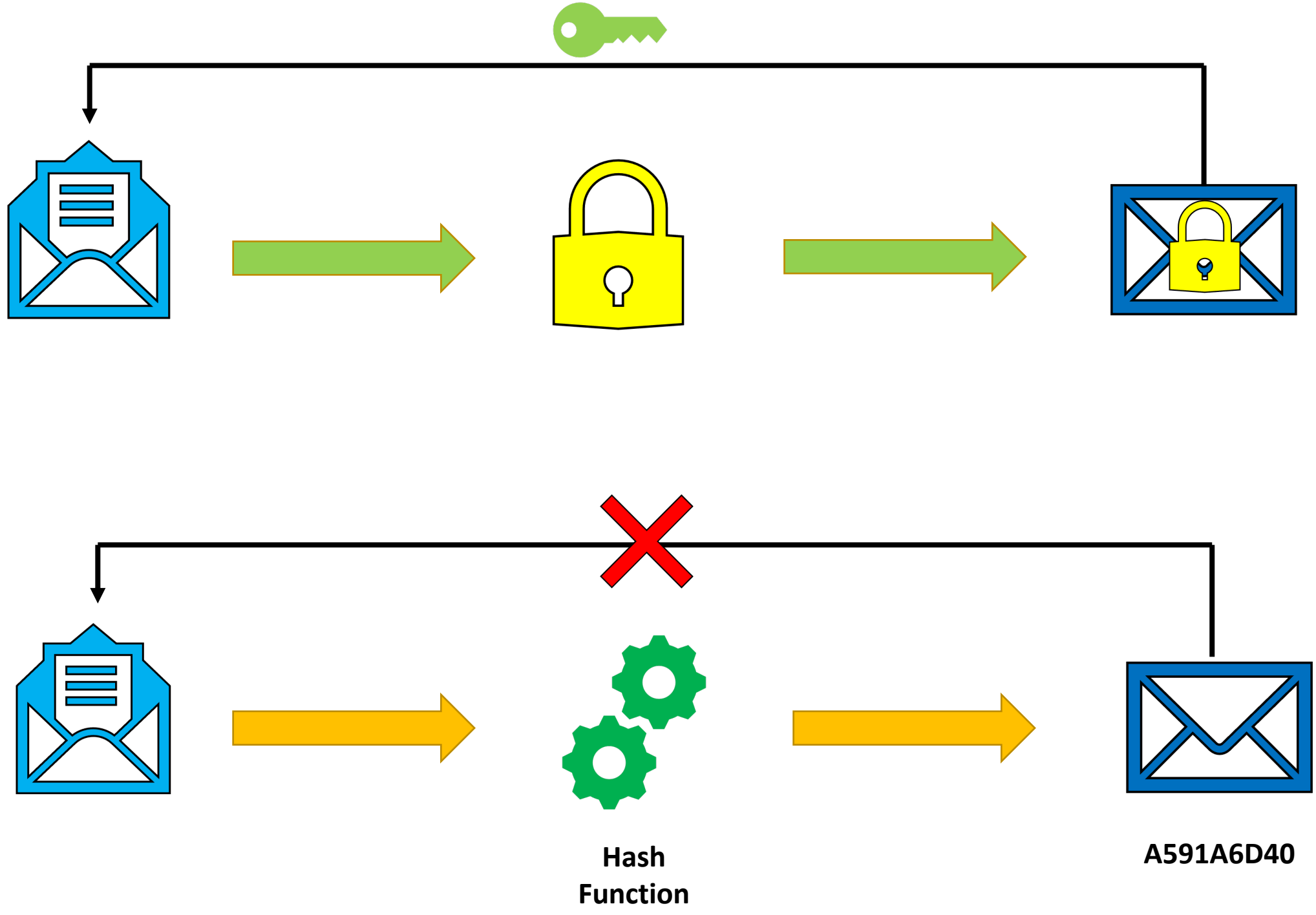
ХЭШ
Функция



SHA256

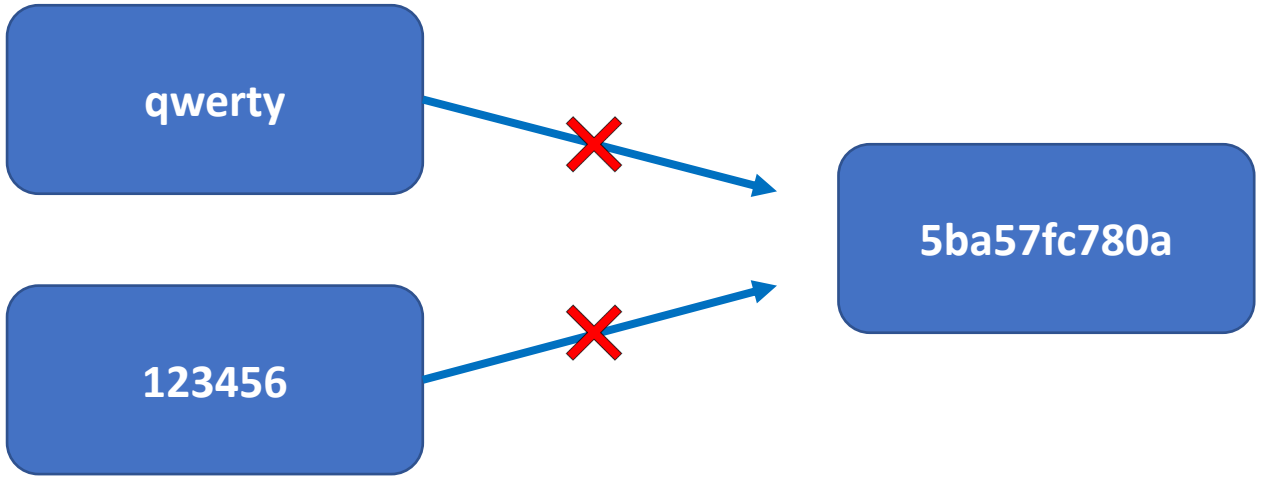
Hello World A591A6D40BF420404A011733CFB7B190D62C65BF0BCDA32B57B277D9AD9F146E


Hash
Function
A591A6D40

Фиксированный размер получаемого ХЭША

Исходное значение	Hash
abc	900150983CD24FB0D6963F7D28E17F72
abc123	E99A18C428CB38D5F260853678922E03
abc123456	0659C7992E268962384EB17FAFE88364
abc123456789	1722442B586A85C95593A9C6131A0EBD
abc123456789123	ED773A76E2CD873AE0C323B28971EBB5
abc123456789123456	5A34EEDB0FC5F5A57E1BF6071608B403

Уникальный хэш и отсутствие коллизий



Наличие лавинного эффекта

Hello World

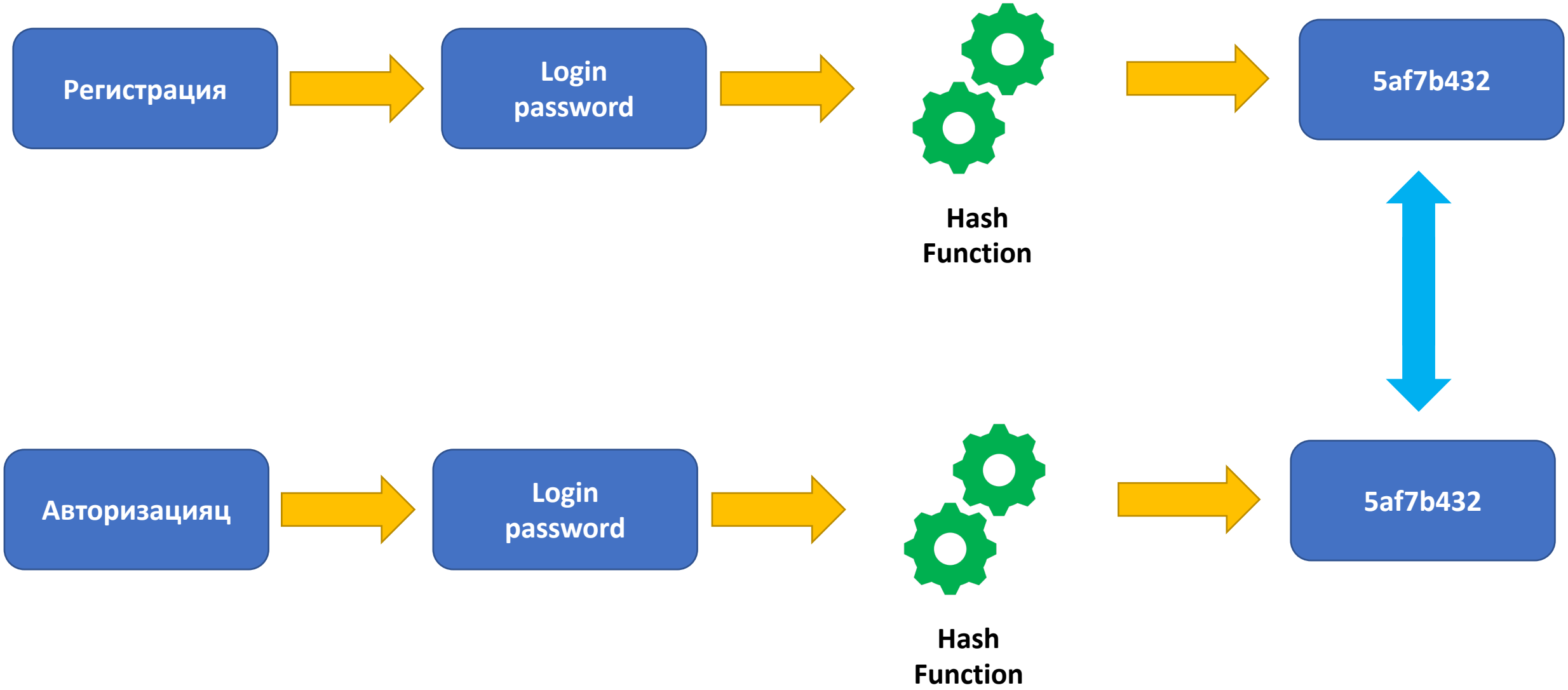
A591A6D40BF420404A011733CFB7B190D62C65BF0BCDA32B57B277D9AD9F146E

Hello World

A591A6D40BF420404A011733CFB7B190D62C65BF0BCDA32B57B277D9AD9F146E

Свойства идеальной криптографической ХЭШ-функции:

- ✓ Детерминированность
- ✓ Высокая скорость хэширования
- ✓ Однонаправленность
- ✓ Наличие лавинного эффекта
- ✓ Отсутствие коллизий


Регистрация
Login
password
Hash
Function
5af7b432
Авторизацияц
Login
password
Hash
Function
5af7b432

Радужные таблицы

Password	Hash
123456	LRHZAFVUZM
qwerty	R6JTUOGLUG
letmein	YB14YN8280
iloveyou	CARPNNFlJW
654321	4LEJZ8EBB5
mypassword	EAHY7W8LH7
trytohackme	G6GP9LMT99

Users	Hash
User1	YY9J3lES8K
User2	HTOjXKSLBG
User3	CWBQB3R5G
User4	EGPR20YLY5
User5	CARPNNFlJW
User6	PJLJQDRVCO
User7	CH28YHE5IQ

Соль

Боб

Password = qwerty + 3olP0Auvtl

Hash = 7E57BDFA3FED4ED1C0561D1A68865A26

Алиса

Password = qwerty + g2tS6Uo3De

Hash = 19D31DEE2320B2101A4AFE76338A7663

The 50 Most Used Passwords

1. 123456	11. 123123	21. mustang	31. 7777777	41. harley
2. password	12. baseball	22. 666666	32. f*cky*u	42. zxcvbr
3. 12345678	13. abc123	23. qwertyuiop	33. qazwsx	43. asdfgh
4. qwerty	14. football	24. 123321	34. jordan	44. buster
5. 123456789	15. monkey	25. 1234...890	35. jennifer	45. andrev
6. 12345	16. letmein	26. p*s*y	36. 123qwe	46. batma
7. 1234	17. shadow	27. superman	37. 121212	47. soccer
8. 111111	18. master	28. 270	38. killer	48. tigger
9. 1234567	19. 696969	29. 654321	39. trustno1	49. charlie
10. dragon	20. michael	30. 1qaz2wsx	40. hunter	50. robert

crackstation.net

SHA256 Hash of your string:

65E84BE33532FB784C48129675F9EFF3A682B27168C0EA744B2CF58EE02337C5

Enter up to 20 non-salted hashes, one per line:

```
65E84BE33532FB784C48129675F9EFF3A682B27168C0EA744B2CF58EE02337C5
```

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
65E84BE33532FB784C48129675F9EFF3A682B27168C0EA744B2CF58EE02337C5	sha256	qwerty

Brute-Forse Attack

bcrypt

scrypt

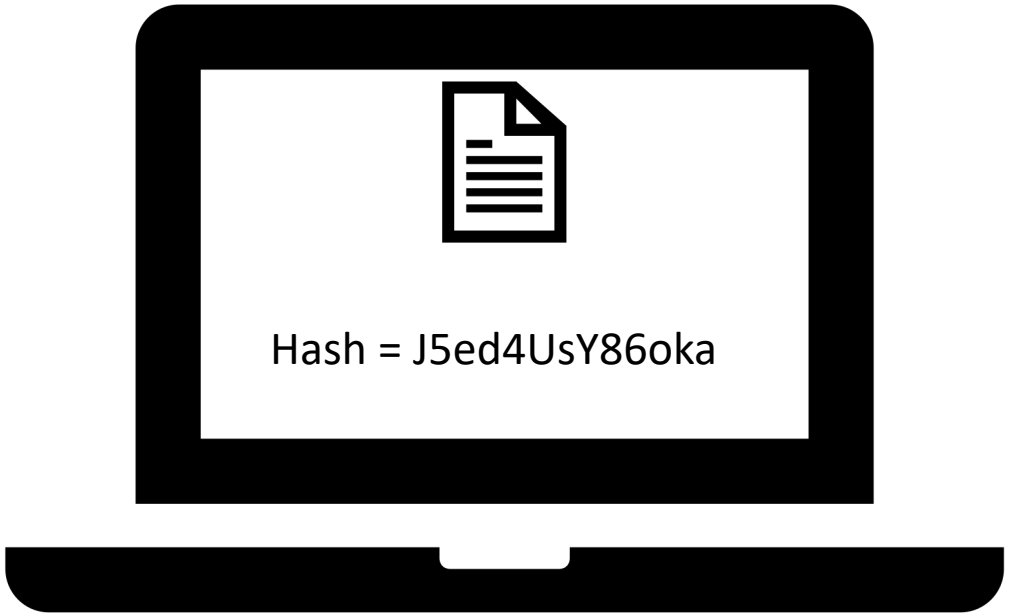
argon2

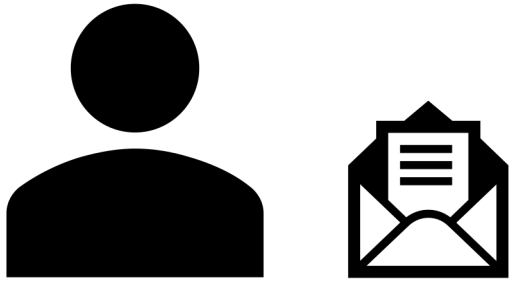
bcrypt

Password(qwerty) + salt(J3kd9UdwS) + cost(10)

DropBox

Проверка целостности файлов





Hash = J5ed4UsY86oka

Коллизионная атака