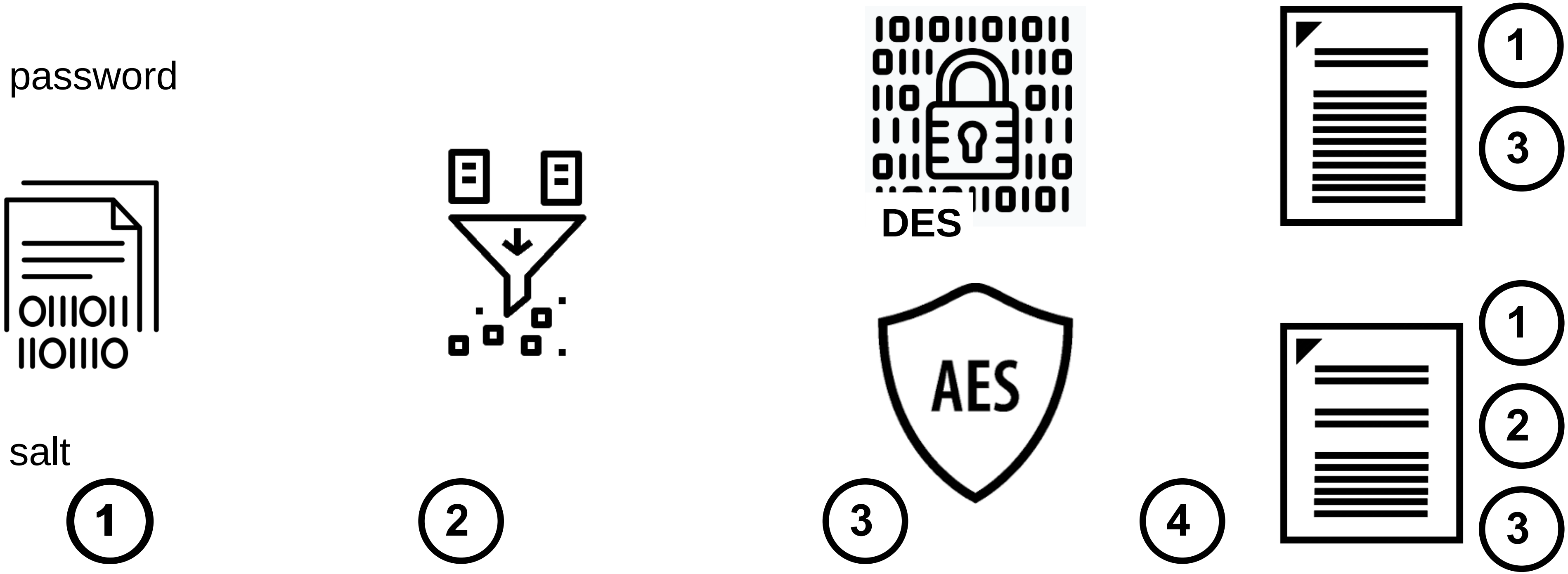
Password-Based Cryptography



password

salt

1

2

DES

AES

3

4

1

3

1

2

3

Password-Based Cryptography Process

- password and salt concatenated
- result is repeatedly hashed producing derived key
- payload is CBC-encrypted with derived key and IV
- prepend salt and IV to encrypted message
- base64 encode the result

Underlying Algorithms

	DES	AES256
MD5	🟩	
SHA1		🟨
SHA512		🟩

🟩 🟩 Perl, Python,Java,.Net

🟨 Perl, .Net