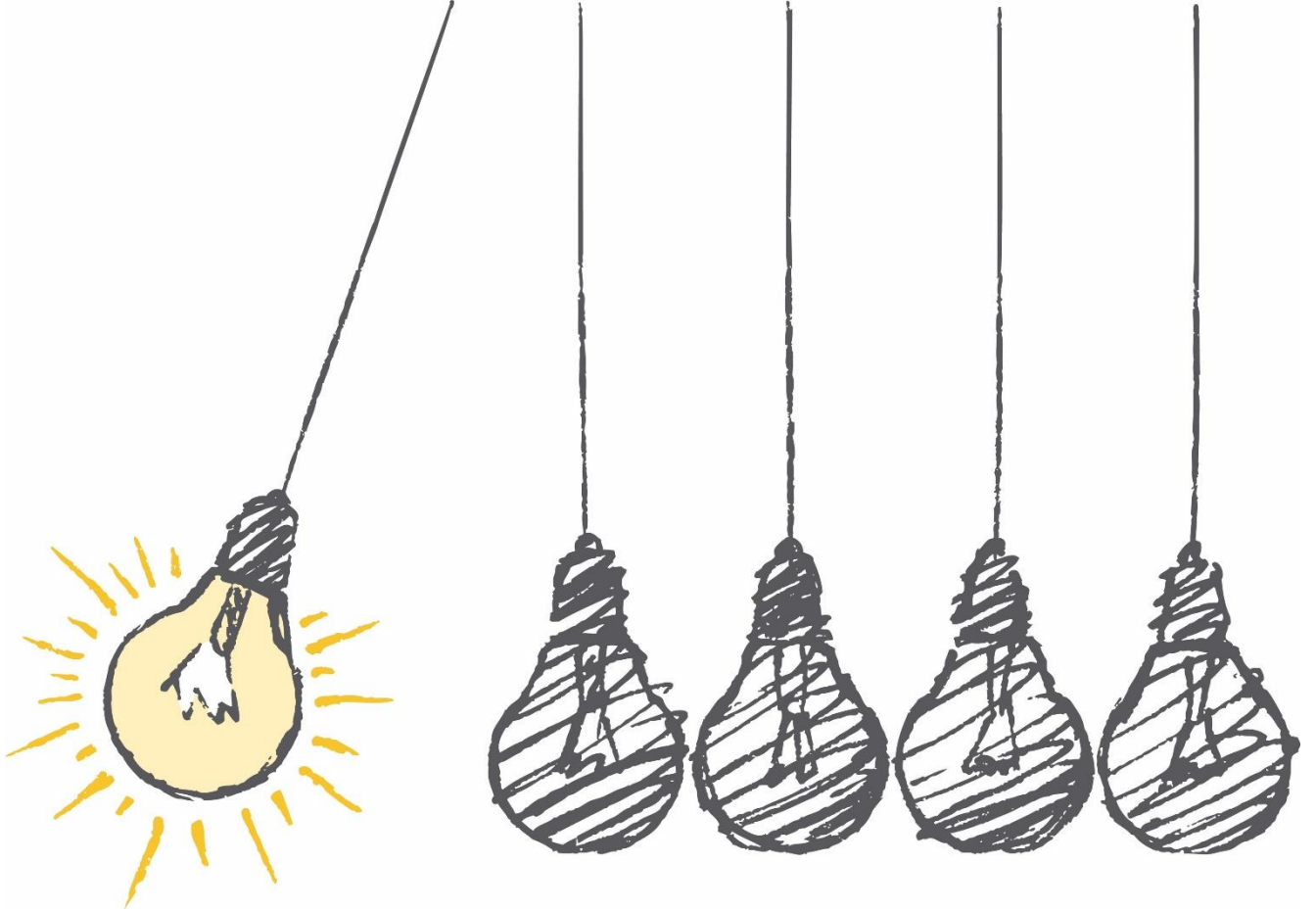
DIME analytics



An intuition for encryption

DIME Bootcamp – Data Security

WORLD BANK GROUP

UKaid from the British people

Norad

Introduction

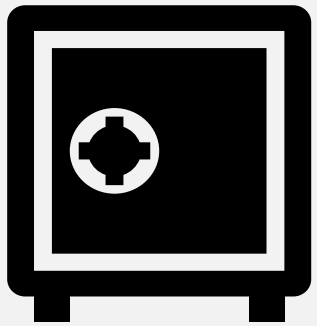
Encryption is a system

- Encryption is only as strong as it weakest link
- Just because your data is encrypted at one point does not meant that your full work flow is properly encrypted
- You can never point to a single file and say, look my data is encrypted and think that is a proof of proper encryption

3 types of encryption

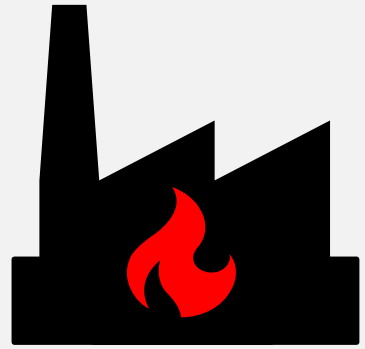
We will not get technical, but there is one way of differentiating encryption algorithms that a researcher should know

Symmetric encryption



Asymmetric encryption

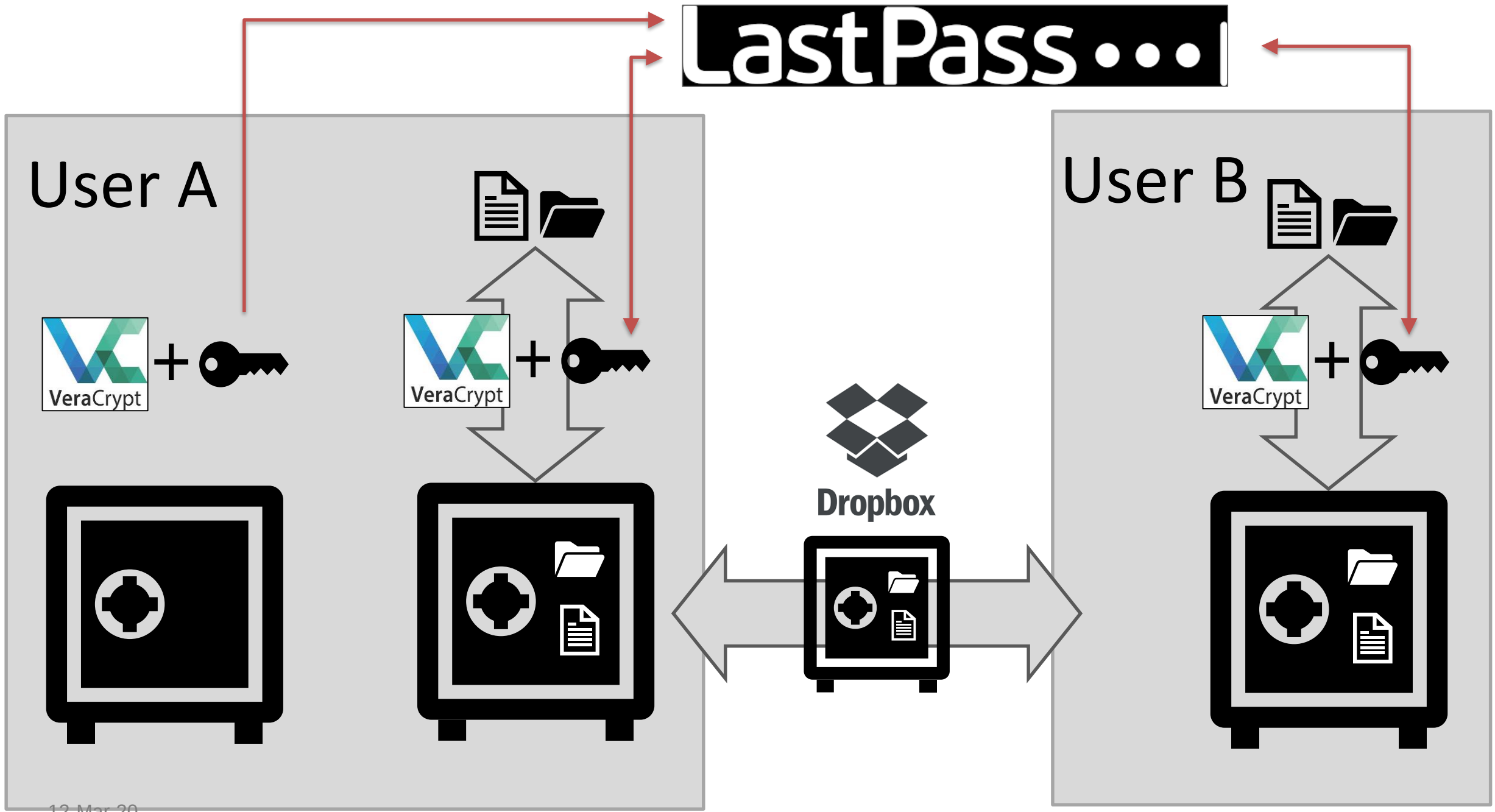
One-way hashing



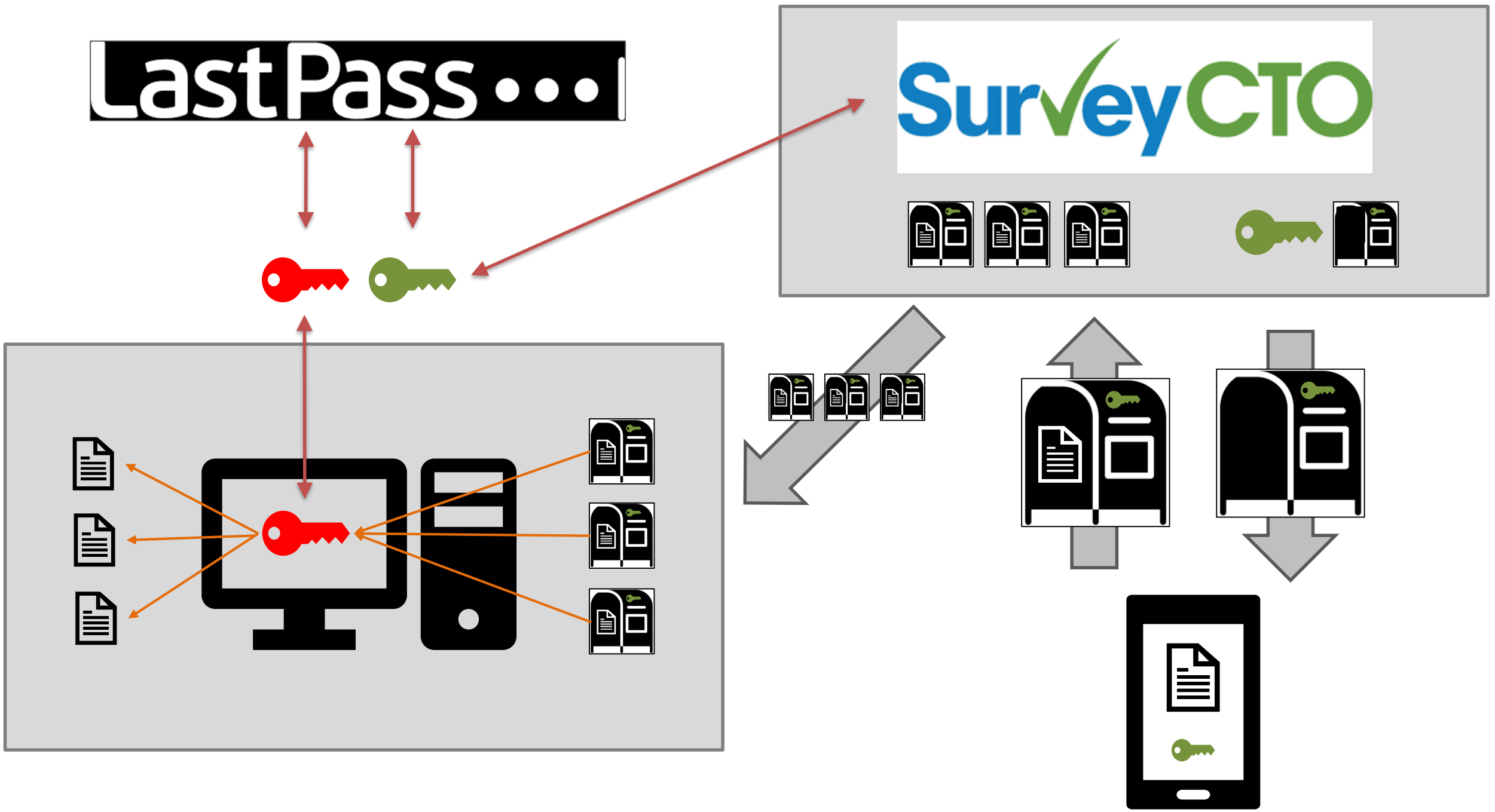
Overview of 3 types of encryption

Type of encryption	Number of keys?	Can it be decrypted?	Real life comparison	Typical use case
Symmetric encryption	1	Yes, with the same key	A physical safe, for which one or many people have the keys to access it's content	Files that are shared and collaborated on
Asymmetric encryption	2 public/private key pair	Yes, using the other key in the key pair	A mail box where anyone can drop a letter but only the postal worker can access the content	Sending data from tablets in the field to our computers
One-way hashing	N/A	No	An incinerator that burn your document, where the ash created is exactly the same each time, if the document was the same	Secure storage of passwords in data bases

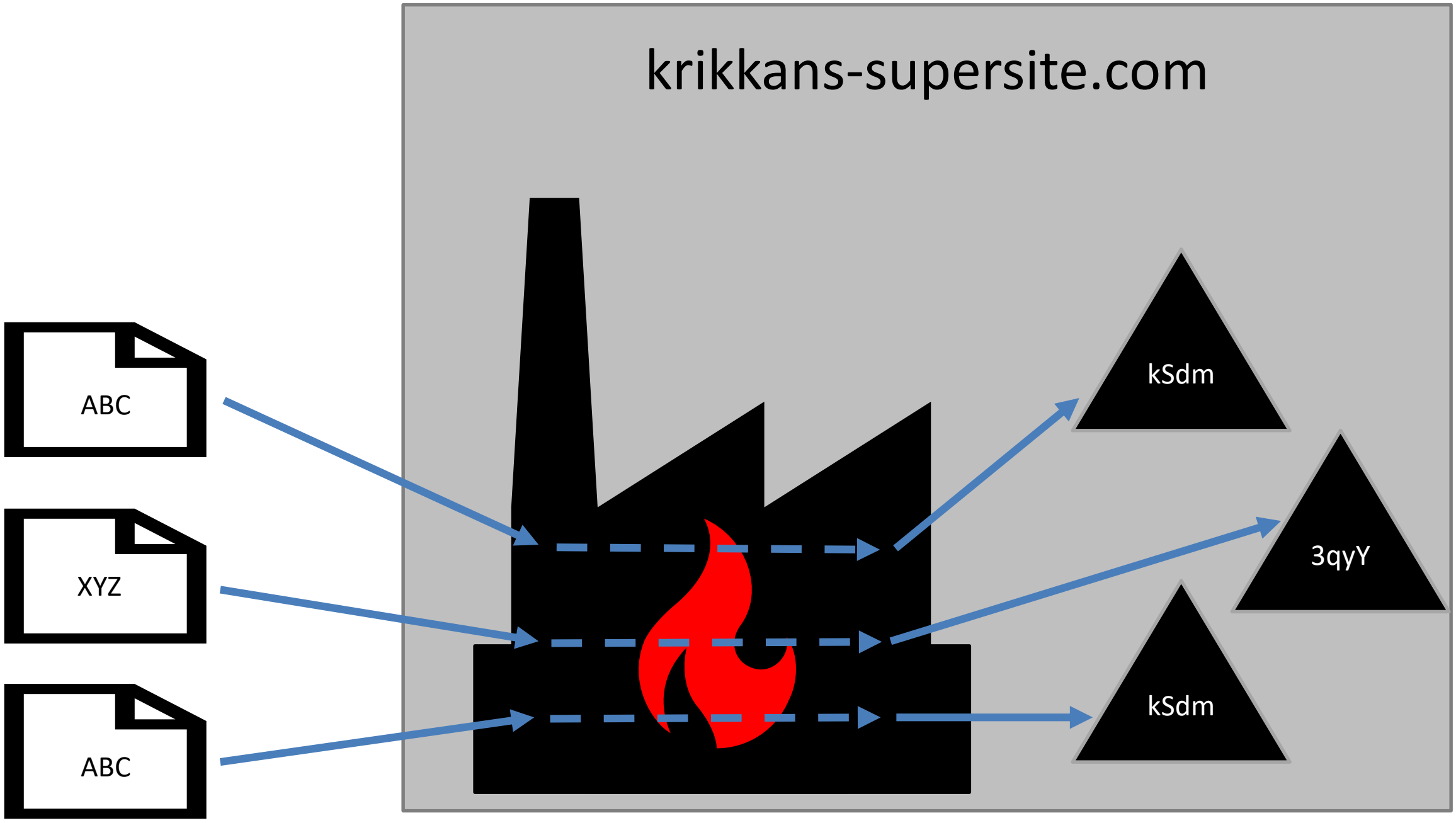
Symmetric Encryption


LastPass
User A
User B
VeraCrypt
VeraCrypt
VeraCrypt
Dropbox

Asymmetric encryption

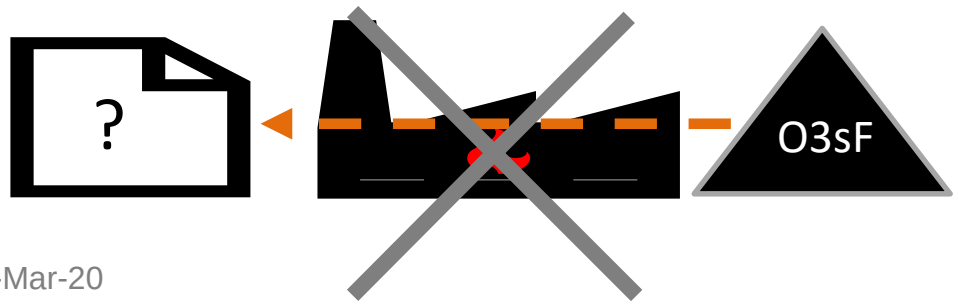

LastPass
SurveyCTO

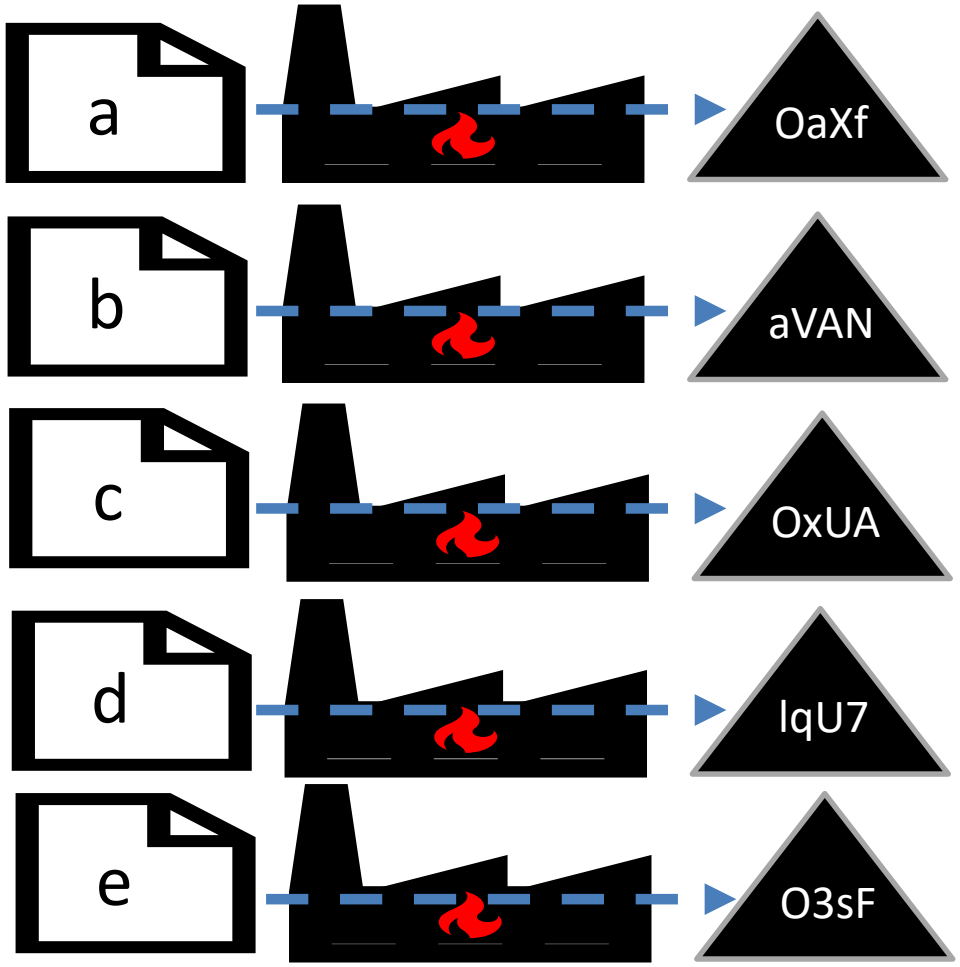
One-way hashes


krikkans-supersite.com
ABC
XYZ
ABC
kSdm
3qyY
kSdm

Cracking hashed passwords

- Let say your password is only the letter “e”
- Your password hash is leaked – its “O3sF”
- Hackers can soon figure out which hashing algorithm was used
- Even when that is known, it is impossible to reverse the hash





Thank you!

Questions?