SUMMARY

113

Comparing data

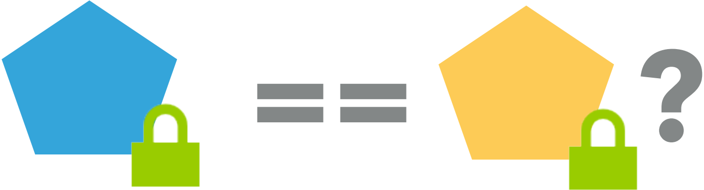
Transparent encryption

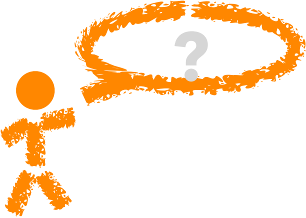
Storing data

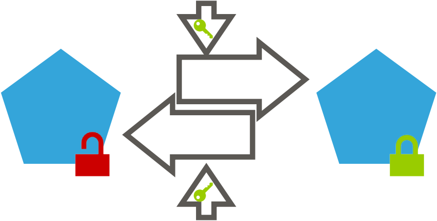
Key derivation

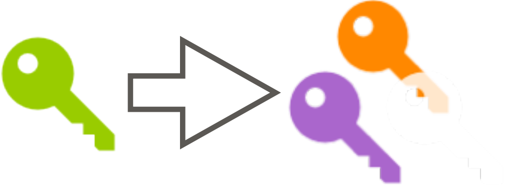
Key refresh

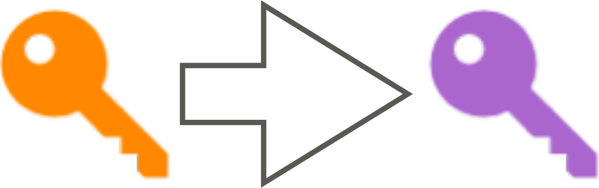
Algorithm rollover









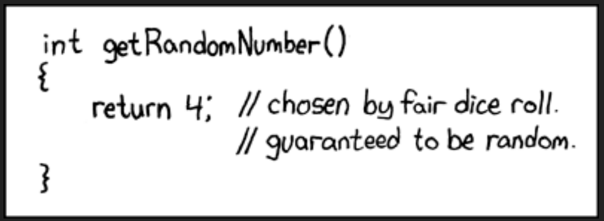


DES	BLOWFISH	AES
MD5	SHA-1	SHA-256
RSA-1024	RSA-2048	?? POST QUANTUM ??

SUMMARY

Integrity

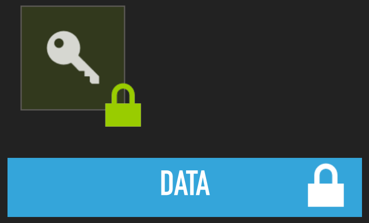
Moving Data



```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Entropy

Access Control



- ☑ Data treatment …
- ☑ Use existing …
- ☑ …

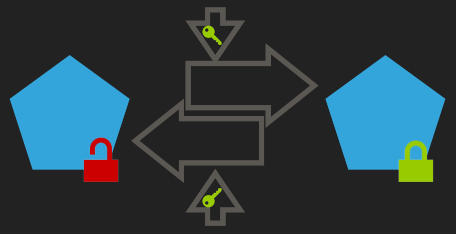
Crypto Checklist

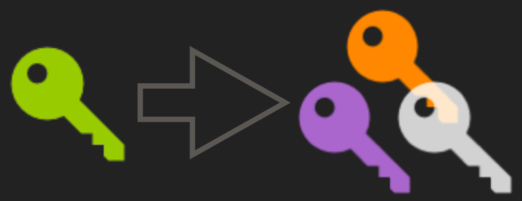
SUMMARY

Comparing data

Transparent encryption

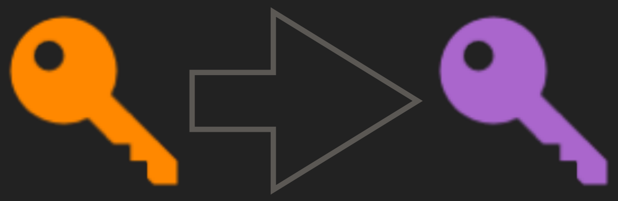
Storing data

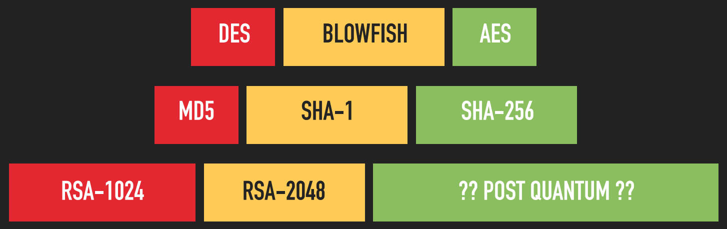




Key derivation

Key refresh





DES BLOWFISH AES

MD5 SHA-1 SHA-256

RSA-1024 RSA-2048 ?? POST QUANTUM ??

Algorithm rollover