



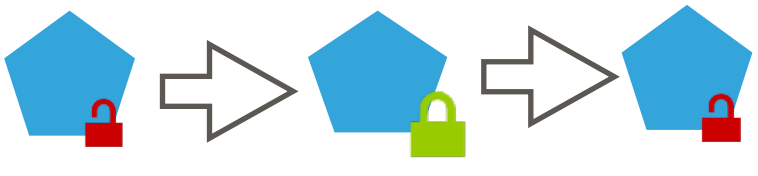
PATTERNS

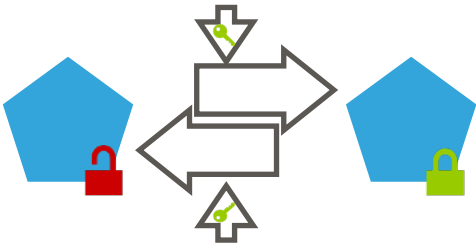
CONTENT
ENCRYPTION



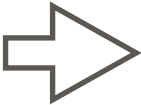
3

8









☒ Data treatment ...

☒ Use existing ...

☒ ...

DES

BLOWFISH

AES

MD5

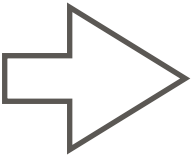
SHA-1

SHA-256

RSA-1024

RSA-2048

?? POST QUANTUM ??





0X123456...



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



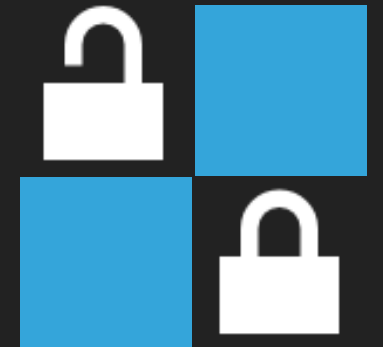

DATA



* * * * *







**MOST IMPORTANT ADVICE:
GET AN EXPERT OR AT LEAST
READ AND UNDERSTAND THE DOCUMENTATION!**

Like all power tools: Better RTFM than to lose an eye!

- ▶ At least be able to explain: "Hash vs. encryption", "Integrity vs. encryption", "Stream vs. block", "Mode of operation", "IV", "Nonce", "Padding", "Key derivation"
- ▶ Identify and name your trust anchors



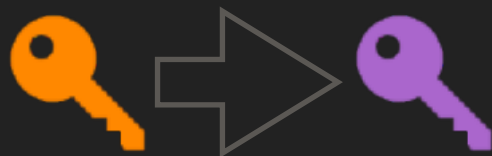
DES	BLOWFISH	AES
MD5	SHA-1	SHA-256
RSA-1024	RSA-2048	?? POST QUANTUM ??

- ☒ Data treatment ...
- ☒ Use existing ...
- ☒ ...



0X123456... ✓

CONTENT ENCRYPTION



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

PATTERNS

