Key length and Key n-bit security

- RSA has very long keys, 1024, 2048 and 4096 are common
- ECC has shorter keys, 256 and 448 are common
- Is it more secure than symmetric crypto with key lengths of 56, 128, 192, 256 ?

➡ Key lengths **do not compare !**

RSA	ECC	Effective key length
1,024		80
2,048		112
3,072	256	128
4096		140
15,360	448	224 ~ 256

Asymmetric vs Symmetric

	Symmetric	Asymmetric
pro	Fast	No key agreement
cons	Key agreement	Very slow

The best of both worlds

- Use asymmetric encryption to encrypt a shared key (or hash)
- Use symmetric encryption to encrypt message

$$E_{Kp}(m) = RSA_{Kp}(k), AES_k(m)$$

Naive approach