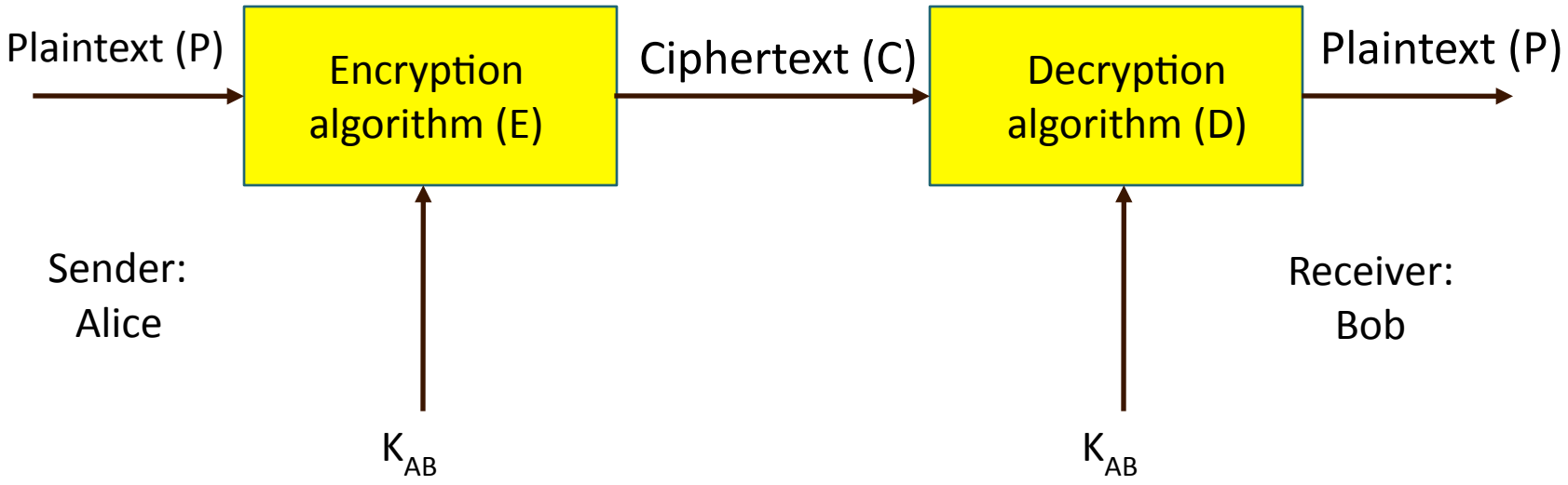
Week 4
Secret Key Cryptography Summary

Secret Key Cryptography



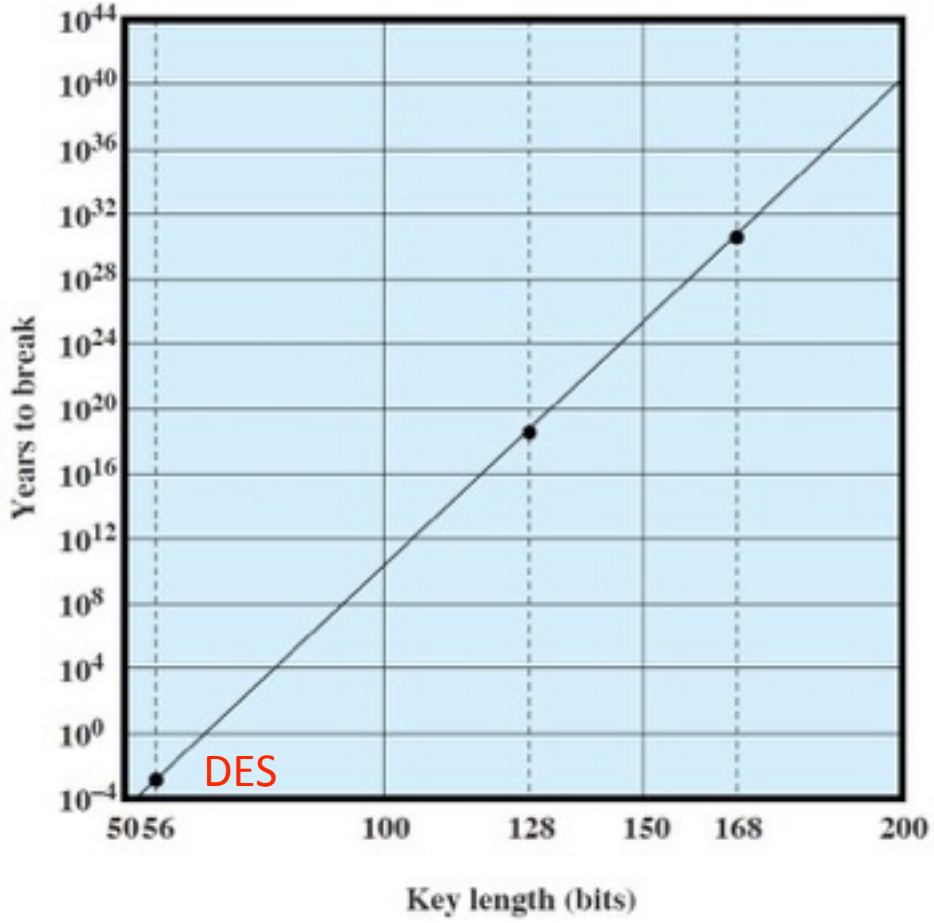
K_{AB}: shared secret key between Alice and Bob

Key Length vs. No. of Possible Keys

Adding one bit to the key doubles the amount of time to crack the key.

Key Length in Bits	Number of Possible Keys
1	2
2	4
4	16
8	256
16	65,536
40	1,099,511,627,776
56	72,057,594,037,927,900
112	5,192,296,858,534,830,000,000,000,000,000
112	5.1923E+33
168	3.74144E+50
256	1.15792E+77
512	1.3408E+154

Time vs. Key Length (Stallings, 2008)



- By a brute force approach assuming 10^6 decryption/µs

- On average, half of all possible keys must be tried to achieve success

Secret Key Algorithms

	RC4	DES	3DES	AES
Key length (bits)	40 bits or more	56	112 or 168	128, 192, or 256
Key strength	Very weak at 40 bits	Weak	Strong	Strong
Processing requirements	Low	Moderate	High	Low
RAM requirements	Low	Moderate	Moderate	Low
Remarks	Can use keys of variable lengths	Created in the 1970s	Applies DES three times with 2 or 3 keys	Today's gold standard, likely to be dominant in the future

Other Secret Key Algorithms

- IDEA (Europe)
- SEED (South Korea)
- GOST (Russia)
- Camellia (Japan)
- Many more

SYRACUSE UNIVERSITY
SUOS
CULTORES
SCIENTIA
CORONAT