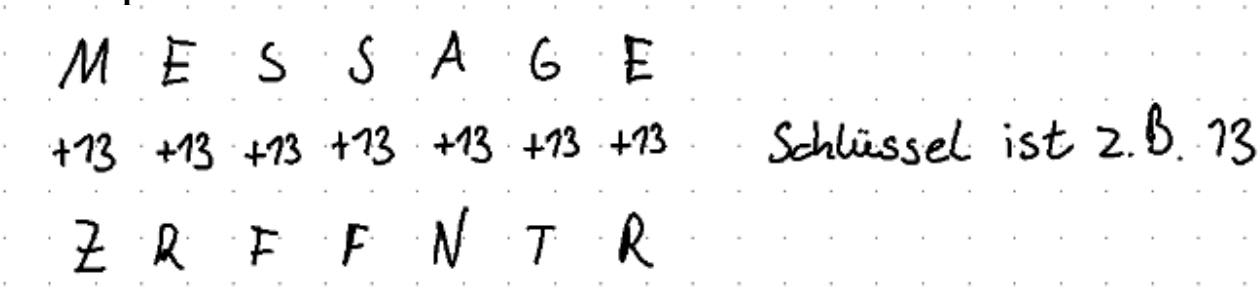
Vigenere (Polyalphabetic)

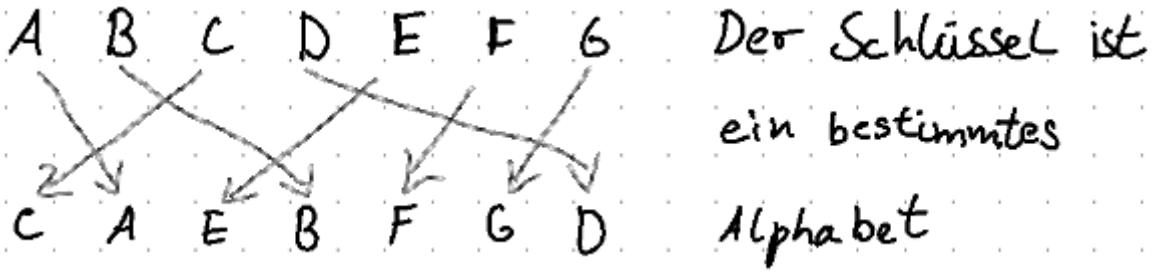
Message	T	H	I	S	A	T	E	S	T
Running key	K	E	Y	K	E	Y	K	E	Y
	+10	+4	+24	+10	+4	+24	+10	+4	+24
Ciphertext	D	L	G	C	E	R	O	W	R

Caesar cipher



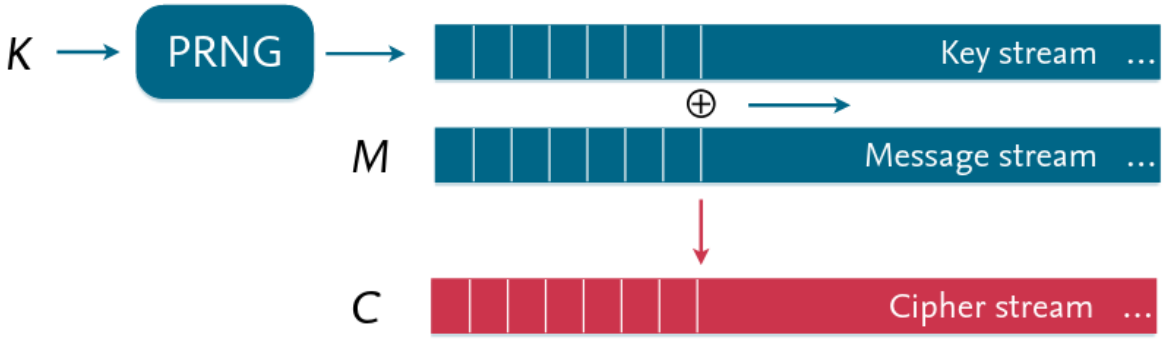
- Keyspace sehr sehr klein

monoalphabetic

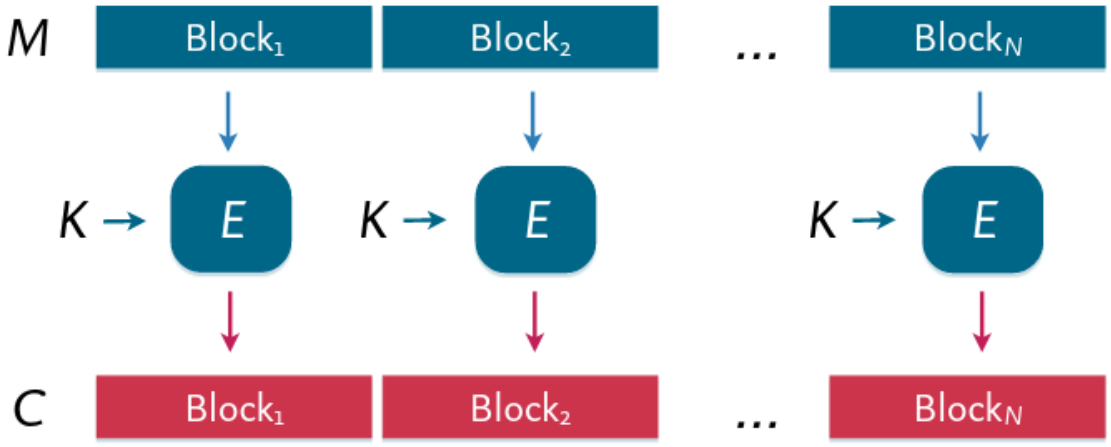


-Zeichenfrequenzen bleiben erhalten
-größerer Keyspace

Stream cipher

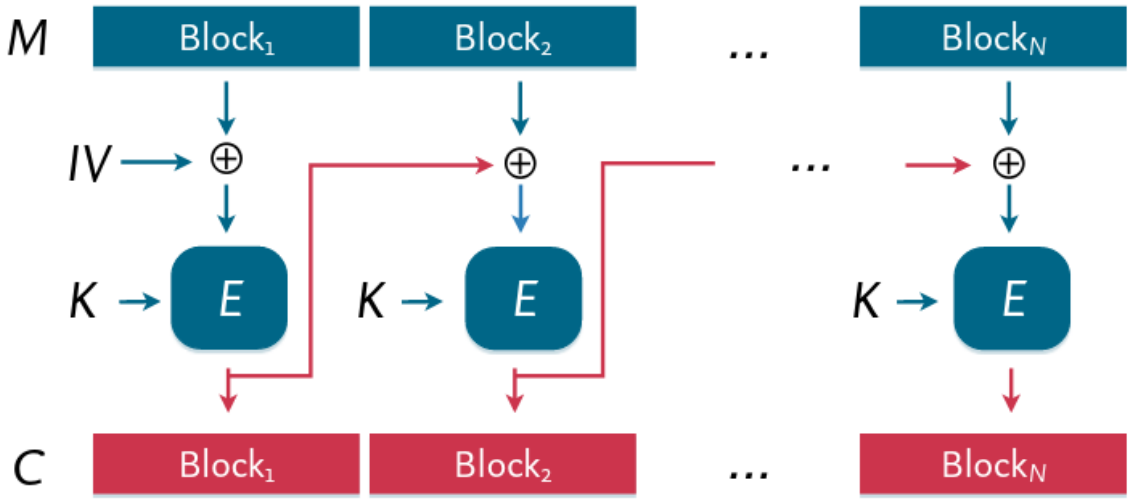


Electronic Code Book (ECB)



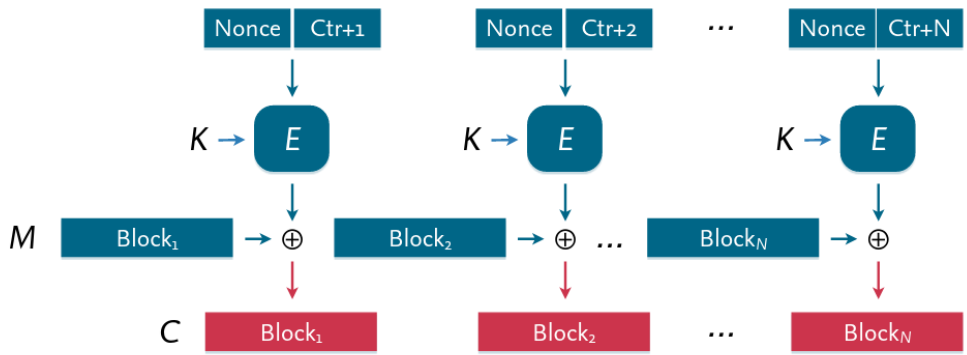
-vulnerable to known plaintext and replay attacks

Cipher-Block Chaining (CBC)



-Chaining of cipher blocks using XOR operator
-(Largely) resistant against known-plaintext and replay

Counter Mode (CTR)



-Auch als Stream-cipher benutzbar (bei ausreichend vorberechnung von encrypteter Nonce+Ctr)
-gut parallelisierbar (keine abhängigkeit zum vorherigen block)
-erneute Übertragen einfach möglich (mit Counter zurück gehen)
-keine Replay Attack möglich