Evolution of cryptosystems

Substitution ciphers
(a.k.a mono alphabetic ciphers)

➡ Improvement over Caesar cipher

Algorithm : allow an arbitrary permutation of the alphabet

Key : set of substitutions

Key space : 26! possible substitutions (4x10^{26} ~ 89 bits)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	K	V	Q	F	I	B	J	W	P	E	S	C	X	H	T	M	Y	A	U	O	L	R	G	Z	N

```
if we wish to replace letters
WI RF RWAJ UH YFTSDVF SFUUFYA
```