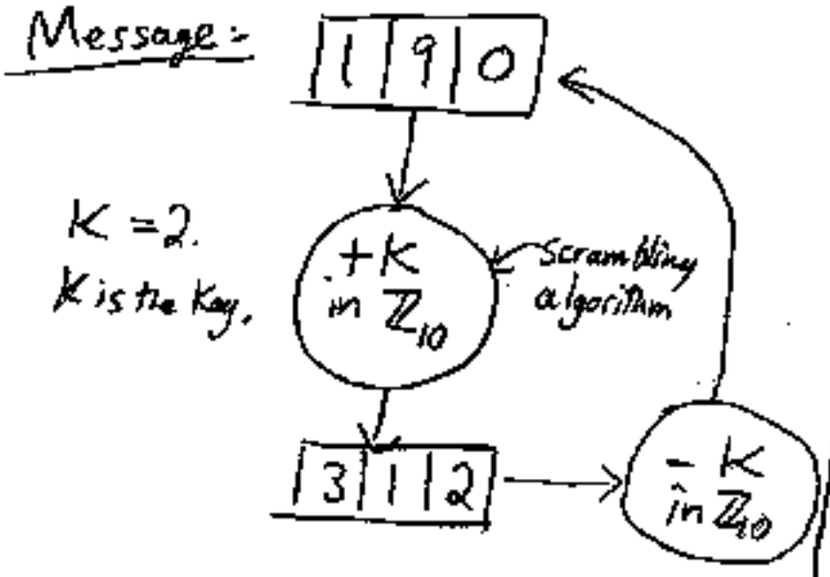
Lecture Notes. Cryptography.

Assumptions:
1. Zero-information assumption
2. Public modulus ($\mathbb{Z}_n$ is known)
3. Public algorithm



Attacker's knowledge:
Everything but K!
The system is "secure" because attacker must try at most ALL VALUES POSSIBLE FOR K. (BRUTE FORCE ATTACK).

Linear cipher. Take message i send to $ax+b$ in $\mathbb{Z}_n$.
a must be invertible i.e. $a \in (\mathbb{Z}_n)^*$.
Then decryption is $(j-b) \times a^{-1}$.

In public-knowledge, want to increase security by maximizing largest possible key-search brute force algorithm length.

Size of BFKS is at most $n \times \varphi(n)$. (Why?)
(n for b, $\varphi(n)$ for a.)

Maximize $n \times \varphi(n) \Rightarrow n \times (n-1)$ (when n prime)

Work on block-sizes for scrambler (permutation).

Vary linear parameters by blocks.

Permutation BFKS worst case? Block size $k \Rightarrow k!$

Perm/Lin on "k" blocks, S lin, & Perm $\Rightarrow |BFKS| = S \times k! \times n \times \varphi(n)$
("k" = block length; with known block size!).