Can GAs be used for cryptanalysis for a substitution cipher, without knowing the key length?

- Considered key lengths from 5 to 15 letters long
- Generated 10 random keys for each length
- Paired off keys of equal length. For each pair: performed crossover, mutated both children
- Select n fittest children and make them the new population
- Ran encrypted text samples on baseline algorithm and my algorithm, compared absolute error of key suitability
- My algorithm outperformed baseline in terms of key suitability – it is possible to recover a keyword without knowing key length

Keyword	Fixed	Fitness	Variable	Fitness
substitution	substitutiln	.3898	subsqitution	.3803
keyword	keyword	.3924	keyword	.3924
algorithm	amgoritlm	.5030	blgorithm	.3916
class	class	.3924	class	.3924
ucfknightsrule	ucgknightjruhp	.5692	uccknightsrule	.3830

Above: Fitness of recovered keys for Lincoln's Inaugural Address with fitness of .3924

Right: Average absolute error of recovered key fitness for all texts

Text	Fixed	Variable
1	.03364	.10398
2	.06746	.01298
3	.05334	.03454
4	.07184	.01968
5	.12954	0.0
6	.05800	.00446