

weak ciphertext failure rate (β)

2^{-21}
 2^{-41}
 2^{-61}
 2^{-81}
 2^{-101}
 2^{-121}
 2^{-141}
 2^{-161}

2^0 2^{36} 2^{72} 2^{108} 2^{144} 2^{180} 2^{216} 2^{252} 2^{288}

work to generate one weak sample ($1/\alpha$)

- no extra info
- 1 ciphertext
- 2 ciphertext
- 3 ciphertext

