Project D.C.

National **I**nstitution of **C**auliflower **H**ealth **E**xamination

May 2019

1 Background

During our centuries of cauliflower examination work, we've noticed that cauliflowers seem to be able to communicate with each other through something like Morse code, by flapping their leaves.

We recorded many samples of communications between cauliflowers over the years. However, even our best linguists cannot make any sense out of it. The entropy is just too high.

2 Long Lasting Research

In year 1924, jazz musician George Myers pointed out that the messages that the cauliflowers are sending to each other might be encrypted.

Although he wasn't able to provide any significant proof, it created a cauliflower research boom.

The **N**ational **I**nstitution of **C**auliflower **H**ealth **E**xamination (**NICHE**) has always been the pioneer of cauliflower research. In year 1940, **NICHE** founded **Project D.C**., where **D.C.** stands for "**D**ecrypting **C**auliflowers".

Every year, tons of taxpayers' money goes into this project. Although very little progress (if not none) has been made for most of the year, the government has been very supportive of this project consistently.

3 Breakthroughs

The first breakthrough was made in year 1969, when mathematician John Waterman had a dream about cauliflowers teaching him textbook RSA. He immediately jumped off the bed and started reviewing those intercepted messages as RSA encrypted messages.

The result was shockingly promising. Those messages do indeed resemble many characterics of an RSA encryption. For example, every message is at most 2048 bits. Sometimes,

they pass pairs of numbers that looks like RSA key pairs around (A large 2048-bit number and a relatively smaller number).

Finally in year 1997, neurosurgeon Louis Walker discover the key generation algorithm of the cauliflowers while dissecting one. It is indeed very similar to a normal RSA key generation algorithm, except for the fact that they always try to satisfy one constraint when choosing their **P** and **Q**s. That is,

$$A \times P \approx B \times Q$$

to be precise, the difference between $A \times P$ and $B \times Q$ is less than 10000, where

$$1 \leq A, B \leq 1000$$

That's a huge breakthrough! At least we are proud to say that we did not waste that thousands of years of taxpayers' money.

4 Current Status

While we've made very impressive and fascinating discoveries, we are not yet able to decrypt what the cauliflowers have to say.

5 Next Steps

The next step is of course trying to break the RSA key pair and decrypt the message that the cauliflowers are constantly sending out.

We sincerely believe that, with the advancement of science and technology, ~~as well as the increase in taxes,~~ human and cauliflowers will soon be able to understand each other.