

# Assignment 10

Michael Lee

CCST9017 - Hidden Order in Daily Life: A Mathematical Perspective

University Number 3035569110

Tutorial Group 009

November 16, 2018

**Question Q. 1.** Thoughts on PGP

**Answer Q. 1.**

I am totally agree with his statements.

The first reason is that privacy should be regarded as a basic human right. No one should be allowed to ever infiltrate others' secrets by using any method, even the government. We don't go naked out the street because of privacy, We are not allowed to get inside others' home, even polices cannot, for the same reason. And this human right should be always regarded, no matter it is a physical or electonical media, unless it is legal to steal things on internet but robbing others' house remain a crime.

The second reason is handling privacy to total control of government is highly dengerous, both in a political and techincal sense. Techincal, a government that stores tons of keys of citizen maybe a highly valuable target to hackers , considering that most of the best hackers won't choose to work in government, these keys will proably got stolen by those highly intelligent guys. We can't put the stake of our privacy, which could mean business, into an unsafe situation. In a political sense, it is highly possible that governments which holds the true power, use their ability without legal authorization, or even use it for the leaders' own political good. How can we trust them? Snowden has already expose that this is actually happening.

**Question Q. 2.** Use Fermats little theorem to find the remainder when  $2^{123}$  is divided by 29.

**Answer Q. 2.**

Since 29 is a prime number, we have

$$2^{28} \equiv 1 \pmod{29}$$

hence we have

$$2^{123} \equiv 2^{28 \times 4 + 11} \pmod{29} \quad (1)$$

$$2^{123} \equiv (2^{28})^4 (2^{11}) \pmod{29} \quad (2)$$

$$2^{123} \equiv 2^{11} \pmod{29} \quad (3)$$

$$2^{123} \equiv 2048 \pmod{29} \quad (4)$$

$$2^{123} \equiv 18 \pmod{29} \quad (5)$$