6G5Z3006 NUMBER THEORY AND CRYPTOGRAPHY

Options talk by Dr Killian O'Brien

MMU, February 2017

THE UNIT

- Number Theory (Dr Killian O'Brien)
- Cryptography (Dr Jon Borresen)
- 3 hours lecture + 1 hour tutorial per week
- Coursework problems (30%), Examination (70%)
- Popular unit (49 students in 14/15) with good ISS results

IN A NUTSHELL

Number Theory

- The study of the integers
$$\mathbb{Z} = \{\cdots - 3, -2, -1, 0, 1, 2, 3, \ldots\}$$
- Of fundamental importance are the primes
$$2, 3, 5, 7, \ldots$$
- Nice mixture of proof oriented theoretical work and algorithmic methods

Cryptography

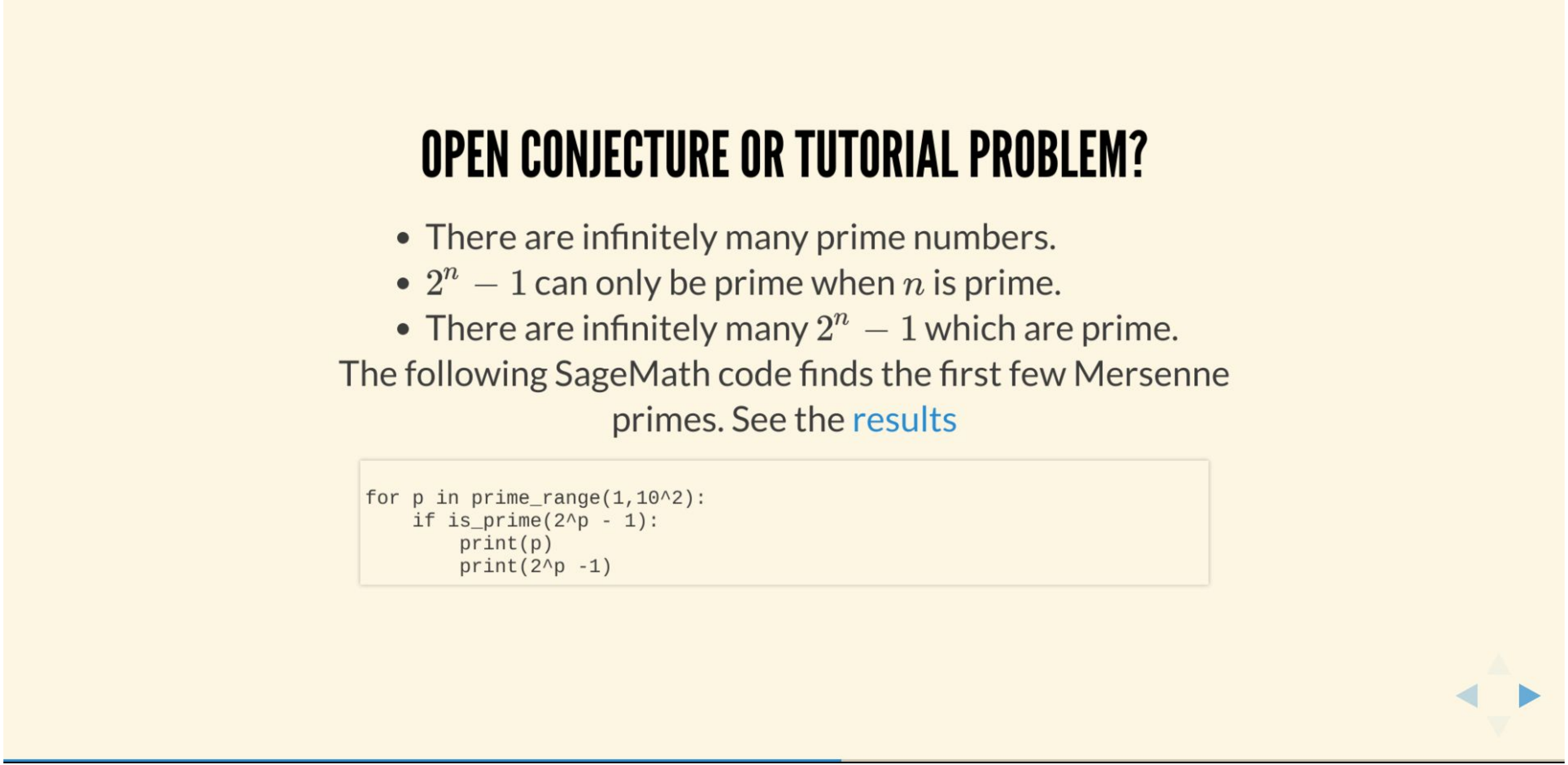
- The science/art of transforming *text* so that it can only be *read* by selected recipients.
- Often in connection to military/industrial/political/...

A QUICK TOUR OF SOME HIGHLIGHTS FROM THE UNIT

INTEGERS IN THE NEWS

What's so special about ... ?

- $74,207,281$
- $2^{74,207,281}-1$

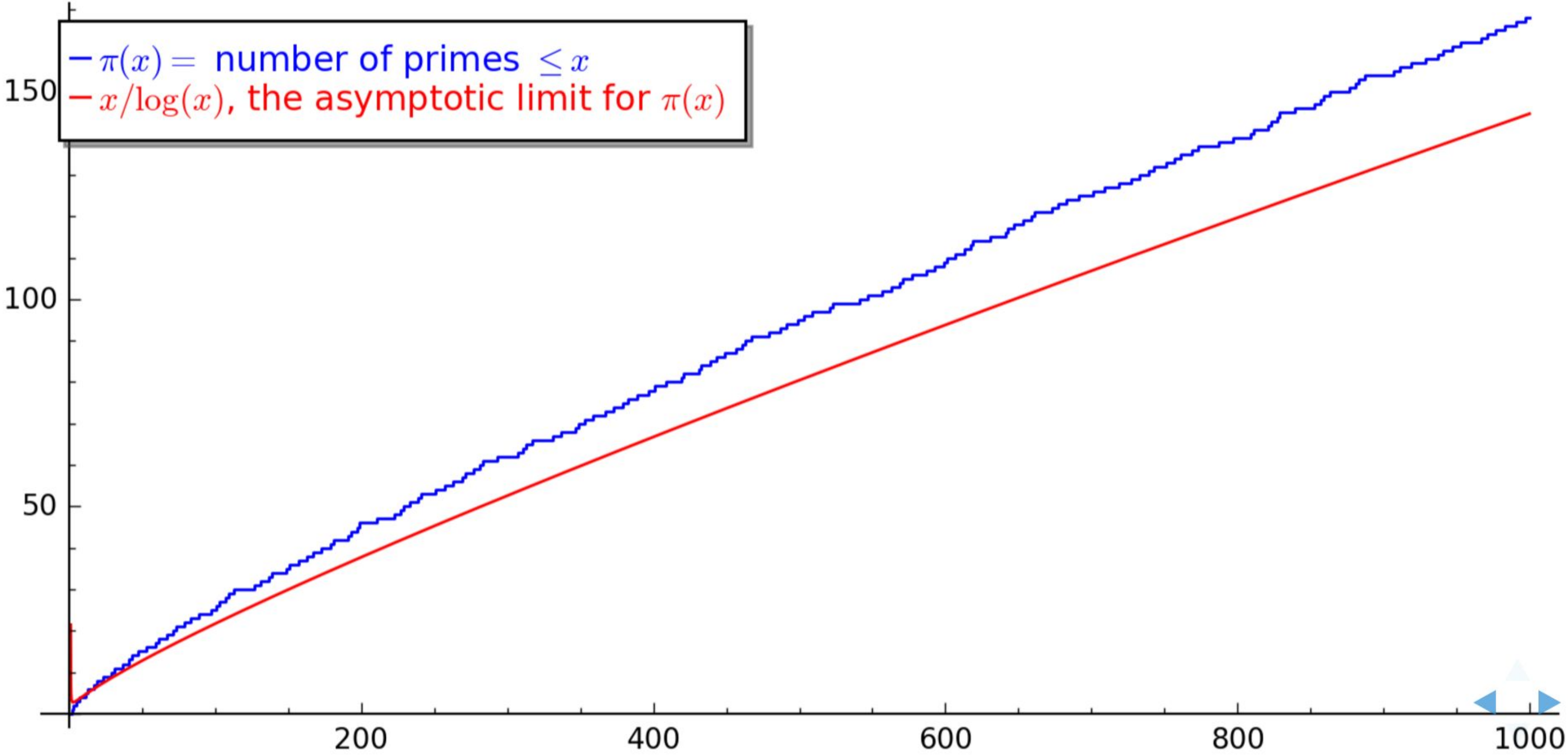


OPEN CONJECTURE OR TUTORIAL PROBLEM?

- There are infinitely many prime numbers.
- $2^n - 1$ can only be prime when n is prime.
- There are infinitely many $2^n - 1$ which are prime.

The following SageMath code finds the first few Mersenne primes. See the results

```
for p in prime_range(1,10^2):
    if is_prime(2^p - 1):
        print(p)
        print(2^p -1)
```


— $\pi(x) =$ number of primes $\leq x$
— $x/\log(x)$, the asymptotic limit for $\pi(x)$
150
100
50
200
400
600
800
1000

OPEN CONJECTURE OR TUTORIAL PROBLEM?

- There are infinitely many primes p for which $p + 2$ is also prime, i.e. *narrow* steps on the π staircase.
- For any integer $n \geq 1$ there are infinitely many gaps of at least length n between consecutive primes, i.e. *wide* steps on the π staircase.

CLASSICAL VS. MODERN CRYPTOGRAPHY

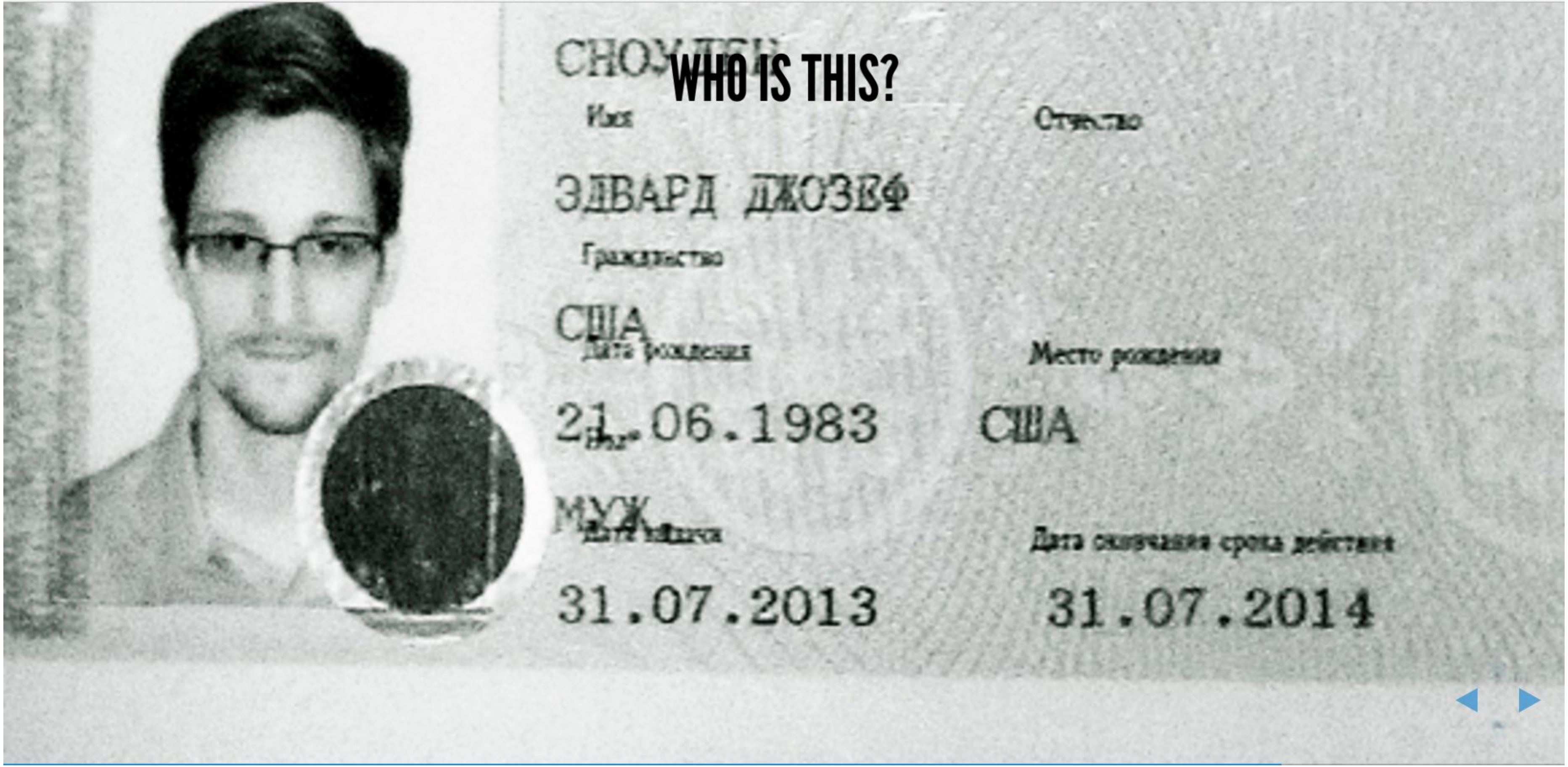
Classical

- Topics include mono- and poly-alphabetic substitution ciphers.
- Classical cryptography required prearranged secrets between sender and recipient.
- Can be broken with the aid of frequency analysis and these vulnerabilities.

Modern

- Crypto systems based on number theoretic concepts.
- Prearranged secrets no longer required, so called *Public Key Cryptography*.

WHO IS THIS?



СНОУДЕН

Имя

Отчество

ЭДВАРД ДЖОЗЕФ

Гражданство

США

Дата рождения

Место рождения

21.06.1983

США

Пол

МУЖ

Дата выдачи

Дата окончания срока действия

31.07.2013

31.07.2014

WHO WAS THAT?

- Edward Snowden, former worker for the CIA and NSA.
- In 2013, he fled the USA, briefly staying in Hong Kong before securing temporary asylum in Russia.
- Has passed many thousands of classified files from the NSA, GCHQ and other intelligence agencies to journalists.
- These revelations concern global surveillance programs carried out by these agencies on the public.

CITIZENFOUR MOVIE

How did Snowden make secure contact with journalists he had never met?