Crittografia a chiave pubblica: uno sguardo alle vulnerabilità di RSA e Diffie-Hellman

Leonardo Alfreducci

Relatori
Dott. Gaspare Ferraro
Prof.ssa Anna Bernasconi

Università di Pisa
Dipartimento di Informatica

Pisa, 7 ottobre 2022

Table of Contents

Section 1

Introduzione

Introduzione

- Lo scambio di informazioni di ogni tipo avviene attraverso la rete: è dunque di fondamentale importanza proteggere le informazioni che vengono scambiate
- Si passeranno in rassegna i protocolli RSA e Diffie-Hellman (su campo primo e su curve ellittiche)

Lorem ipsum

- First item
  - Sub item
- Second item
- Third item

Lorem ipsum

1. First item
2. Second item
3. Third item

La complessità è $O(\sqrt(n))$

$$O(n) \tag{1}$$

Listings

```c
#include <stdio.h>

int main(void) {
   printf("Hello World\n");
   return 0;
}
```