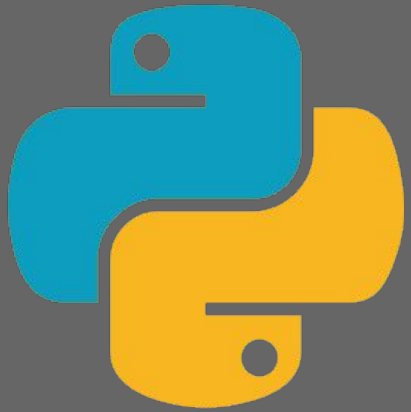
ICMC USP
SÃO CARLOS

GANESH

Python

A linguagem de programação

- Features modernas
- Tipagem dinâmica
- Ótima para prototipagem e scripting



Conceitos Básicos

- Tipos de dados
  - Inteiros
    - Tamanho arbitrários
  - Float
  - String
    - Não existe diferença de char e string

Operações Básicas

- Aritméticas
  - Soma, subtração e multiplicação agem como o esperado
  - A divisão quando não inteira casta para float
    - Diferente de C
    - Se usar // vira divisão inteira
  - Tem também potenciação com **
  - Soma e multiplicação funcionam com strings

Operações Básicas

- Lógicas
  - Usa-se and e or para as operações lógicas
  - Usa-se &, | e ^ para as bitwise

Tipagem

- Dinamicidade de tipos
  - Um nome em python não precisa ficar preso sempre ao mesmo tipo
- Tipagem forte
  - Porém python não nos permite misturar tipos

Entrada e Saída

- Lê-se usando o input()
  - Essa entrada é lida como uma string, necessário cast para ler inteiros ou floats
- Imprime-se usando o print
  - Cada argumento por padrão é separado por um espaço e no fim tem um \n
  - Para alterar a separação basta passar um valor para sep
    - print(saida1, saida2, sep=”*”) separaria com *
  - Para alterar o final você deve passar um valor para end
    - print(saida1, end=””) não tem o \n

Listas

- Conjunto ordenado de objetos
- Podem ter vários tipos
- Podemos adicionar e remover elementos de qualquer posição
- Soma concatena
- Principais métodos
  - append
  - pop: remove a posição dada
  - remove: remove o elemento dado
  - index: retorna o índice do primeiro elemento encontrado

Strings

- Conjunto de chars
- Em python são imutáveis
- Soma concatena
- Podem ser multiplicadas por números
- Métodos principais
    - len
    - in
    - split

Controle: Condicionais

- if, elif e else
- Sem chaves
- Sem parênteses
- Com : e indentação

Controle: repetição

- While: Funciona como em c
- For: É o que se chama geralmente de foreach
  - Necessita de um iterável (lista, string, set …)
  - Percorre todos os elementos do iterável
  - Range
  - Enumerate
  - Zip

Imports

- Jeito de adicionar bibliotecas em python
- Modo normal: import biblioteca
  - Para usar uma função da biblioteca usa-se biblioteca.func
- import biblioteca as bib
  - Usamos bib.func
- from bib import func:
  - Podemos rodar func diretamente

Pip

- Package manager do python
- Nos permite instalar novas libs
- pip install lib

A biblioteca os

- Permite interagir com o sistema
  - os.system() executa um comando da shell
  - os.uname() retorna informações sobre o os (kernel, nome da máquina…)
  - os.chdir(path) da cd pro path
  - os.chmod(path, mode) dá um chmod no arquivo em path
  - os.getcwd() retorna o diretório atual

A biblioteca Sys

- Acesso a objetos criados ou mantidos pelo interpretador Python
  - sys.argv[] - Argumentos passados para o programa
  - sys.exit([arg]) - Fecha o programa com uma possível mensagem de erro

    …

    Além de várias manipulações de variáveis do Python em si

Pwntools

- Biblioteca para facilitar a exploração de sistemas
  - Dividida em vários fragmentos
  - Abordaremos “Utility e Tubes”
    - Links de referência no final dos slides

Pwntools - Tubes

- Facilitar a comunicação e automatizar recebimento e envios
  - remote(ip, porta) -> Realizar conexão
  - send, sendline
  - recv, recvline, recvuntil
  - clean

Pwntools - Utilities

- Utilitários no geral (por exemplo criptografia)
  - enhex, unhex
  - b64e, b64d
  - bits
  - urlencode
  - md5sumhex

    ...

Referências extras

- Violent Python - A Cookbook for Hackers, Forensic Analysts, …
- Black Hat Python
- Cracking Codes with Python
- Referência de python 2
- Referência de ppython 3
- Referência do Pwntools
- Tutorial Pwntools

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br