Project Two Report

Paul Jayme | 300222932

RSA Challenge – Estimates the strength of an algorithm or application against exhaustive key-search

BlowFish Algorithm – variable key length – symmetric block cipher

“Bag of Tasks” Architecture – single key manager and dynamic set of clients

TWO PROGRAMS: KeyManager and Client – Evaluate Performance

KEY MANAGER:

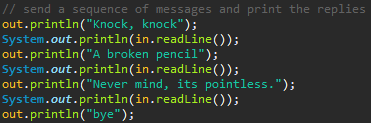
* Handles Clients joining system
* Allocates them key spaces to search & report results
* NO GUI – invoked from CMD Line | java KeyManager initial-key keysize ciphertext
* Initial-key: starting point for the search | integer
* Keysize: defines the key spaces | expressed in no. of bytes
* Ciphertext: text encoded as a base64 string
* Print a RANDOM PORT No. – to be used by clients
* When key has been found – PRINT message on CMD indicating success + PRINT KEY OR FAILURE MESSAGE
* Keep track of how long it takes to either find the key or come to the end of the key space and print this when it exists – TIMER COUNTER

CLIENT:

* Java client

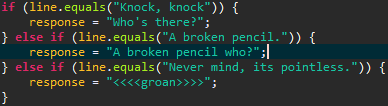
# Task One:

EchoClient.java:

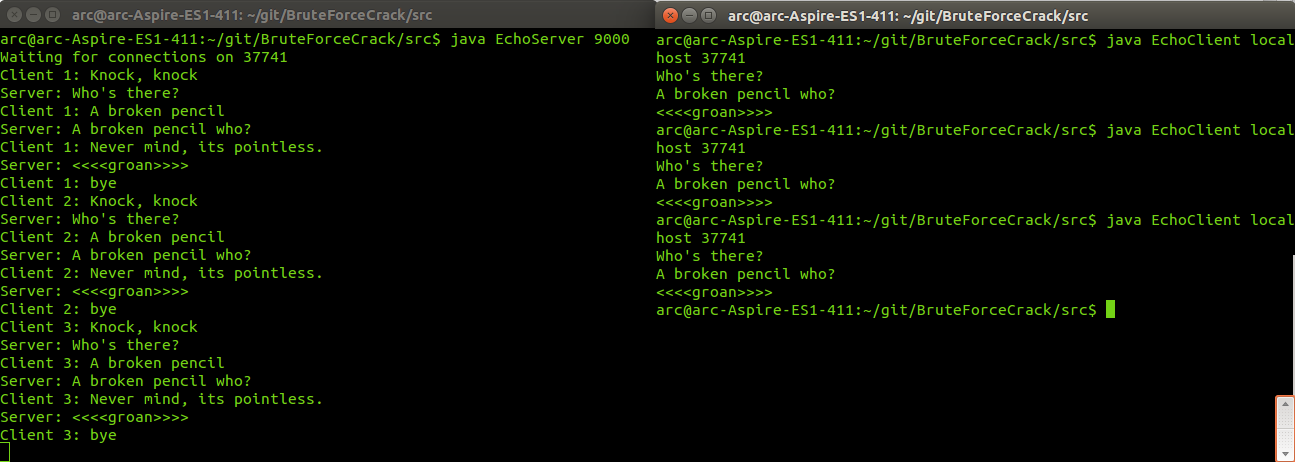


* When an EchoClient is launched it establishes its communication channels then sends a sequence of messages to the EchoServer. Here the code has been modified to a different knock-knock joke. The server must then recognize what the client is saying so it also has to be modified from that end.

Connection.java:

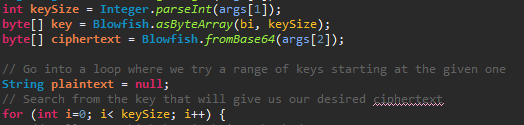


* When a new thread is created by the EchoServer class it uses the Connection class as its main Thread class (since Connection extends Thread). Hence when “Connection.start()” is called, the program executes the “run()” method of the Connection class which launches the knock-knock joke interaction between the client and the server.

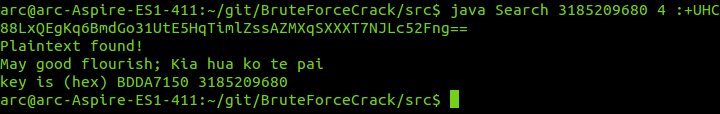


*Above is a screenshot of the system functioning correctly - the left terminal represents the “Manager” / Server who is waiting for connections on port 37741. The right terminal represents the multiple clients that have connected to the Server. The moment a client connects to the server the full interaction is displayed on the terminal of the Server. Ultimately, the sequence of running the system starts with launching the server followed by clients connecting to the server.*

Search.java:



* Search was initially searching based on a fixed number of keys (100 keys) – “i < 100”.
* The conditional statement defined in the for-loop has now been changed to handle a dynamic / user-defined number of keys – “keySize” which is entered as the arguments of the program prior to its launch.



*Above is a snapshot of the Search function working accurately – it finds the correct key based on a user-defined key-size of 4.*

# Task Two: Control Flow & Requirements

## Key Manager:

1. The EchoServer is launched with three arguments – initial-key, key size and cipher text. The server launches on a randomized port and begins listening for incoming connections.

The server/manager is responsible for allocating key spaces for each client (i.e. the range in which each client will search the keys for) and managing the connections of each of these clients.

Upon launch, the user is prompted to enter the total number of clients – this is used to determine the “chunk-size” each client will get. For instance if we had 4 clients with a key size of 4 then there can be 4 billion possible key-variations, so the manager will look to distribute the workload equally across all 4 clients – approx. 1 billion possible key-variations for each client.

Once the server/manager has computed the accurate chunk-size then it creates the “messages” to be sent to the clients. The messages contain three key data-elements which are the “current-key”, “chunk-size” and “ciphertext”. When the client receives the message it begins executing its search.

1. Once the client has finished executing – the Manager will expect to receive results and check to see if the key has been found.
2. When the key has been found, the Manager prints success and the time it took to find the key. Consequently, if the key is not found the Manager prints a failure message.
3. The Manager shuts down once the key has been found or when it has exhausted its key space.

## Client:

1. The Client simply requests for more work each time it has finished executing its task/search.
2. When a client connects for the first time it immediately pings the Server a message stating “Requesting Work..” – the Server then recognizes this and composes a message containing the search parameters and sends this to the client.
3. Once the client has received this message, it proceeds to execute its search
4. Once finished it reports back to the Manager and if the search is unsuccessful then it requests for more work but if it the search returned successful then it kills the processes.

## Requirements:

1. Clients are only connected to one socket which is the ServerSocket therefore it only knows the location of the Server and is completely unaware of the location of the other Clients. The architecture is setup in such a way that the two programs – Server and Client are independent processes. Once the Client has received its designated task from the Server then it independently processes this without relying on other clients.
2. Once a client has joined/connected, the Manager composes a message containing the range of keys that the client will search in along with the cipher text. The architecture guarantees that the client will first return the results of its search before sending a message to the manager that it is ready to request for more work.
3. The clients are built in such a way that once it has finished executing its search it will continuously ping the server to request for more work. The manager is able to compute and decide if there is more work left to do and in what particular key-range should this client be searching in.
4. Messages are only exchanged in two scenarios:
   1. Manager sends the search parameters to the clients
   2. Clients sends results back to the Manager

When a Manager or Client is doing its independent computations i.e. computing the search-range or executing the actual key-search then it is not interacting with any of the communication channels. The programs only use the channels when it has finished performing its computations and has a substantial message to send across the network.

1. When the key is found the Manager prints the key along with the time it took to find the key. Consequently, if the key is not found then it prints a failure message – stating that it has exhausted the key space and also the time it took to do the full search. When any of these scenarios occur the Manager shuts down and all client connections are terminated.

Requirements:

1. Clients only need to be aware of location of Manager
2. Clients can join or leave but will complete the work they have been requested
3. Clients request work from the key manager and return results to it - DYNAMIC
4. Connections between clients and the Masters only exist long enough to request work or to return results
5. When the key is found, the key manager will shutdown

DYNAMIC

1. Client is free – requesting work
2. Manager checks for other threads running
3. Pauses them splits work between free client and current client
4. I.e. pausing client 2 – changing search parameters
5. Client 2 from 0 – 10 , client 3 from 10 -20

First Complete:

* Timer – start when first client connects – finish when key found or key not found
* Printing Accurate Results – success print + fail exhausted key space
* Connection only exists for request and send
* When Key is found send signal to kill all clients