Collective Pattern

CIS 510

Department of Computer and Information Science
University of Oregon

UNIVERSITY OF OREGON

Developer Training

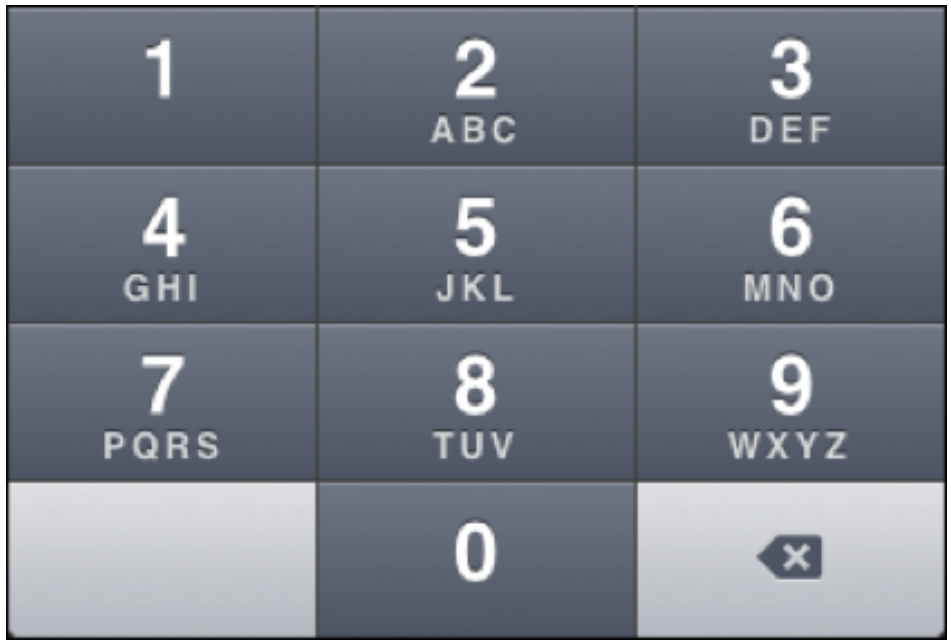
Collective Pattern

Executive Password Recovery

Executive Password Recovery

Our previous weeks' endeavors have emboldened management in their efforts to avoid work

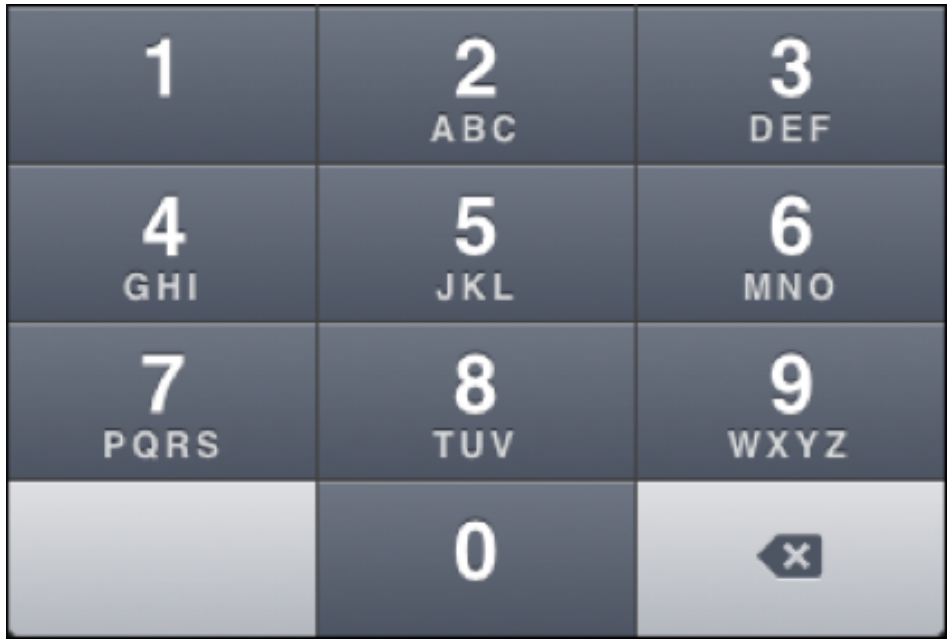
Executives have passwords they must change weekly, these are too valuable to simply be hashed. They must be encrypted by a series of keys stored in a set of undisclosed locations. For this, they will need an encryption tool capable of taking the set of encryption keys and encrypting a password. Having all keys also enables a password to be recovered, preventing management from needing to remember theirs.



Encryption Algorithm - Multi Key Xor

XOR based encryption is a class of encryption algorithms in which the encryption and decryption keys are the same

Each bit of the string is compared to the corresponding bit in a string of key bits for any number of keys. These keys can and will have different lengths, some combinations of key lengths lend themselves to trivial solutions. We will not make things that easy on the aliens. For messages longer than the length of our keys we will cycle back to the beginning of a key when we run out of key bits

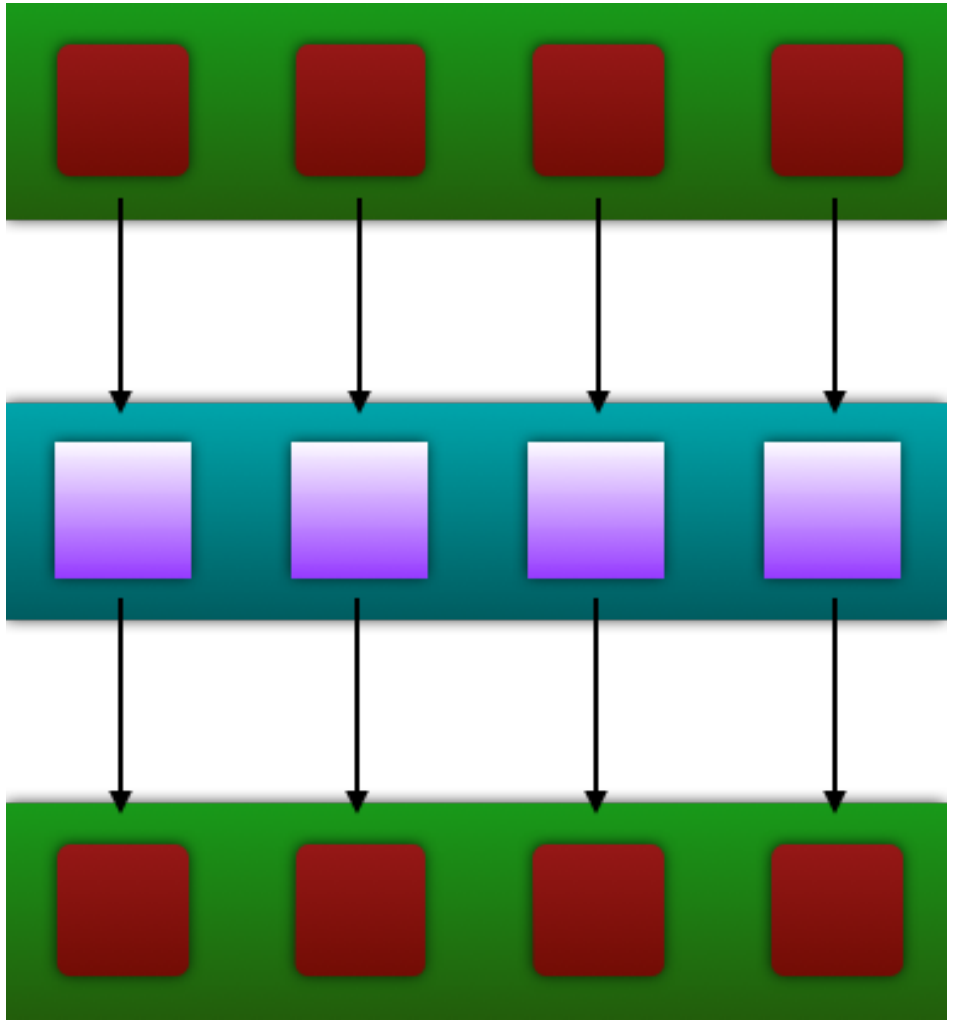


Basic Solution

- You will be provided a password
- Give the software a number of keys to generate
- Software generates the given number of keys
- Software prints plaintext, then prints encoded text, then prints decrypted text to prove results
- `http://ix.cs.uoregon.edu/~dellswor/410`

Collective Reduce Operation

- N atomic data units, one output (a Gather Operation)
- Binary operation applied across inputs to produce the result
- Example: adding all input integers in a list to create output sum
- We will be xor'ing an input bit with a set of key bits to create output bit



Parallel Multiple Key Xor

- Our solution is way too slow
- If only we had a team of developers to parallelize it...

Multiple Passwords - Example code

- Example code is stored on Mist
- Get into a directory you store source in
- On Mist: run "cp -r /home/users/poliadz/OpenmpPasswordCracker ."

Key Points - Map

- Concept: apply the same operation to multiple data elements, producing a single output
- Design: Challenge in map is ensuring operations do the same amount of work
- Identifying the correct parallelization is key to performance