NETWORKS AND CRYPTOGRAPHY — PROJECT 5
Cracking substitution-permutation networks

For this project, you will be given a ciphertext created with a known *substitution permutation network (SPN)* and an unknown key. Your goal will be to use linear and/or differentail cryptanalysis to obtain the key and decrypt the message.

1 Getting the code and ciphertext

To get started, login to one of the CS Department systems and bring yourself to a shell. Then follow these steps:

```
$ cd cs28
$ tar -xzvpf ~sfkaplan/public/cs28/project-5-v3.tar.gz
$ cd project-5
```

You will find a number of handy files here:

- `SPN.java` — The source code of the SPN. Critically, this code will reveal to you the π_s and π_p functions necessary for cryptanalysis. You will also see that, like the sample SPN in class, this one uses three normal rounds of mixing/substitution/permuting, followed by a fourth and final round of mixing/substituting/mixing.
- `SPNWithKey.class` — A pre-compiled version of SPN with a key (*the* key) built into it. When you run this program it only performs encryption, and it does so with the key unknown to you.
- `message.ciphertext` — The encrypted message, created using *the* key built into `SPNWithKey`. This is the message that you need to cryptanalyze.

2 How to submit your work

Send email to me with evidence that you've decrypted the ciphertext correctly.

This assignment is due at **5:00 pm** on **Friday, May 14**—the **last day of exams**