**Name: Nachiket Joshi**

**Cryptography:**

The practice of making a message unreadable by some method is cryptography. A message which has undergone any cryptographic algorithm will require a particular key for that message to be readable. This has always been a method to carry out communication where a message is only intended for a particular recipient.   
We can even term the trivial postal service a form of cryptographic technique. As each post card has a designated address. This address can work as a cryptic key which enables us to deliver the message to only intended recipient.  
  
**Steganography:**

The only difference between cryptography and steganography is that in cryptography you know a message is hiding some meaningful data but in steganography it is not know if the message is hiding in the message.

**A simple overview of one of the cryptographic technique, Symmetric-Key Algorithm:**

This algorithm uses a cryptographic key to encrypt a plain text message. The key can be shared by two or more parties. The keys can be same of we can implement some kind of transformation technique to maintain keys. The key is like a shared secret between two parties.  
However, this same thing of keeping a shared key can be perceived as a drawback for this technique.  
Depending upon the number of bits the algorithms encrypts at a time, There are two variants of this technique.  
**Stream Cipher**: In this, the bytes are encrypted one at a time.

**Block Cipher:** in this, we take multiple bytes to make a block and then apply cryptic technique on that block as one.

**Overview of the Puzzle Idea suggested for the game:**

Above discussed idea can easily be modeled to be implemented as a puzzle in following manner. The common symmetric key that both the parties should have is the pattern that we need to match in the process. Bothe parties will have the common key i.e. the pattern then both parties can view the highly secure message in it which will eventually lead for the player to save the game and win.

A simple block of squarely shaped puzzles will be given to the player to solve. The aim of the player will be two match the given pattern and the pattern on the screen exactly to decrypt the hidden message. This message will eventually lead the attack to fail. The pattern will eventually be working as a encrypting message that was sent from the enemy side which if the player successfully decrypts, will be able to save the city.

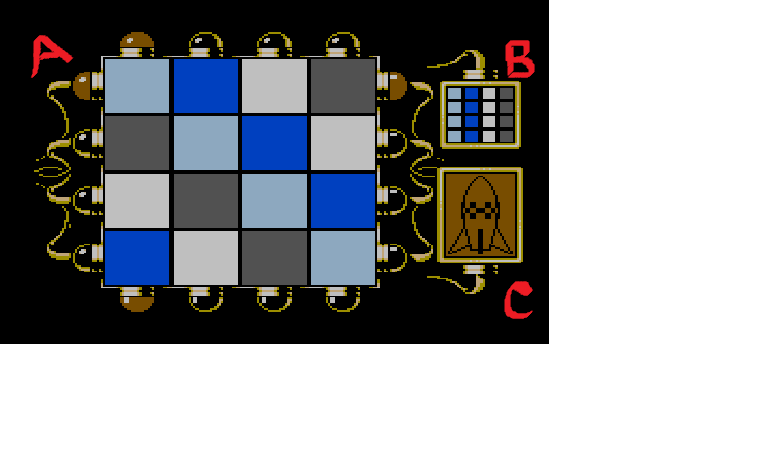
A simple pictorial representation of above puzzle can be like follows,

A small description of labeled parts in the following image,

**1. Lable A:** This will be a simple area given to the player where he can arrange blocks of different colors. The aim will be to match the pattern with the enemy captured message (pattern in the label B)

**2. Label B:** This pattern will be the one that was encrypted from the enemy side and the player has to decrypt it in order to save our city from impending attack.

**3. Label C:** This will have some missile. This missiles launch will be switched off if both the patterns match. This can be modified according to our game design progresses.



These are just crude ideas regarding which puzzled we can model in our game. Extensive discussion, feasibility and other constraints will eventually result in better ideas.

**References for this Document:**

**1. Wikipedia  
2. James Bond NES (nintendo entertainment system) game**