T-79.159 Cryptography and Data Security
2005 / EXAM
Monday, 16 May 2005

1. (6 pts) When the PT-109 American patrol boat, under the command of Lieutenant J. F. Kennedy, was sunk by a Japanese destroyer, a message was received at an Australian wireless station in Playfair code:

   `KX JE YU RE BE ZW EH EW RY TU HE YF SK RE HE GO YF`

   `IW TT TU OL KS YC AJ PO BO TE IZ ON TX BY BW TG ON`

   `EY CU ZW RG DS ON SX BO UY WR HE BA AH YU SE DQ`

   Decrypt the first line. The key used was *royal new zealand navy.* Note that some transmission errors may have occurred.

   If you do not remember how Playfair works you may try to get three consolation points (3 pts) by decrypting the following:

   ```
   M  E  T  J
   A  E  Y  N
   X  H  O  E
   ```

2. (a) (2 pts) What is triple encryption? What is its advantage?
   (b) (2 pts) Why the middle operation in 3DES encryption is decryption rather than encryption?
   (c) (2 pts) What is hybrid encryption?

3. Let $p = 17$, $q = 13$ and $e = 7$ be the parameters of RSA.
   (a) (3 pts) Compute the private key d.
   (b) (3 pts) Decrypt the ciphertext $C = 128$.

4. Consider polynomial arithmetic with polynomial $x^3 + x + 1$ on the set of three-bit integers.
   (a) (3 pts) Determine the discrete logarithm of $6 = \texttt{110}$ to the base $2 = \texttt{010}$.
   (b) (3 pts) Find the multiplicative inverse of $3 = \texttt{011}$.

5. Counter Mode PRNG is also called as Cyclic Encryption PRNG.
   (a) (2 pts) Explain how Counter Mode PRNG using IDEA encryption algorithm works. What size of a counter you would use?
   (b) (2 pts) Given one or more output blocks of a Counter Mode PRNG can you say something about other blocks generated by the same PRNG without knowledge of the secret key?
   (c) (2 pts) For what such a PRNG can be used in a practical security system?