ΑΣΦΑΛΕΙΑ ΣΤΟ ΦΥΣΙΚΟ

ΕΡΓΑΣΙΑ 2024

ΣΤΟΙΧΕΙΑ

ΜΠΕΡΜΠΑΡΗΣ ΝΙΚΟΛΑΟΣ:
ΑΜ3212020146
ΖΑΧΑΡΙΑΣ ΝΙΚΟΛΑΟΣ ΧΡΗΣΤΟΣ:
ΑΜ3212020062

Διδάσκων:
Μαλιάτσος Κ.

Ερώτημα 1:

Δημιουργούμε την σειρά των 100.000 μηνυμάτων που ζητείται.

Ερώτημα 2:

```
Η εντροπία της πηγής είναι: 3.0000 bits
Πιθανότητες εμφάνισης των νέων μηνυμάτων (M'):
    0.0153    0.0158    0.0156    0.0164    0.0162    0.0155    0.0153    0.0160
    0.0154    0.0159    0.0161    0.0148    0.0158    0.0159    0.0158    0.0145
    0.0159    0.0154    0.0153    0.0156    0.0160    0.0155    0.0149    0.0152
    0.0155    0.0159    0.0150    0.0159    0.0152    0.0154    0.0153    0.0159
    0.0154    0.0160    0.0154    0.0156    0.0161    0.0150    0.0155    0.0159
    0.0152    0.0157    0.0155    0.0159    0.0156    0.0161    0.0157    0.0156
    0.0155    0.0155    0.0158    0.0159    0.0158    0.0158    0.0154    0.0159
    0.0157    0.0162    0.0156    0.0160    0.0158    0.0150    0.0162    0.0156
```

Ερώτημα 3:

```
Τα πρώτα 5 μπλοκ μηνυμάτων με CRC-24:
  Columns 1 through 4

    {'001011001011101...'}    {'100101011001010...'}    {'110101111000011...'}    {'111110001000111...'}

  Column 5

    {'010011110110110...'}

Τα πρώτα 5 μπλοκ μηνυμάτων με Hamming κωδικοποίηση:
  Columns 1 through 4

    {'010101001100101...'}    {'011100110101100...'}    {'101010100111100...'}    {'111011101000100...'}

  Column 5

    {'000010001111011...'}
```

Ερώτημα 4:

Οι κώδικες Hamming είναι μια οικογένεια γραμμικών κωδίκων διόρθωσης σφαλμάτων. Μπορούν να ανιχνεύουν σφάλματα ενός και δύο bit ή να διορθώνουν σφάλματα ενός bit χωρίς ανίχνευση μη διορθωμένων σφαλμάτων. Αντίθετα, ο απλός κώδικας ισοτιμίας δεν μπορεί να διορθώσει σφάλματα και μπορεί να ανιχνεύσει μόνο περιττό αριθμό bit σε σφάλμα.

```
Πιθανότητες εμφάνισης των νέων μηνυμάτων με Hamming:
  Columns 1 through 11

    0.0031    0.0022    0.0012    0.0015    0.0008    0.0014    0.0019    0.0014    0.0010    0.0009    0.0022

  Columns 12 through 22

    0.0013    0.0016    0.0022    0.0009    0.0013    0.0003    0.0006    0.0012    0.0005    0.0018    0.0010

  Columns 23 through 33

    0.0006    0.0004    0.0008    0.0015    0.0008    0.0005    0.0007    0.0007    0.0011    0.0013    0.0003

  Columns 34 through 44

    0.0007    0.0013    0.0012    0.0010    0.0011    0.0004    0.0007    0.0019    0.0013    0.0009    0.0012

  Columns 45 through 55

    0.0005    0.0005    0.0014    0.0015    0.0019    0.0025    0.0017    0.0014    0.0013    0.0009    0.0026


  Columns 4,082 through 4,092

    0.0016    0.0018    0.0022    0.0009    0.0017    0.0006    0.0009    0.0013    0.0017    0.0016    0.0015

  Columns 4,093 through 4,096

    0.0014    0.0020    0.0022    0.0016

Η εντροπία των νέων μηνυμάτων με Hamming είναι: 39.1007 bits
Η υπό συνθήκη εντροπία είναι: 36.1007 bits
Η αμοιβαία πληροφορία είναι: 3.0000 bits
```

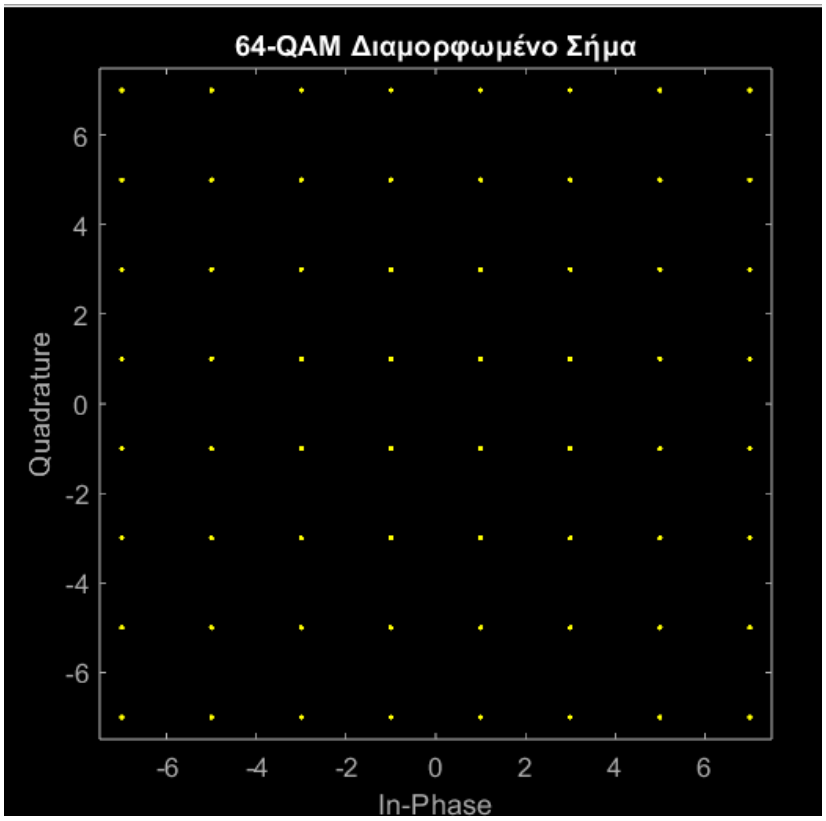
Ερώτημα 5:

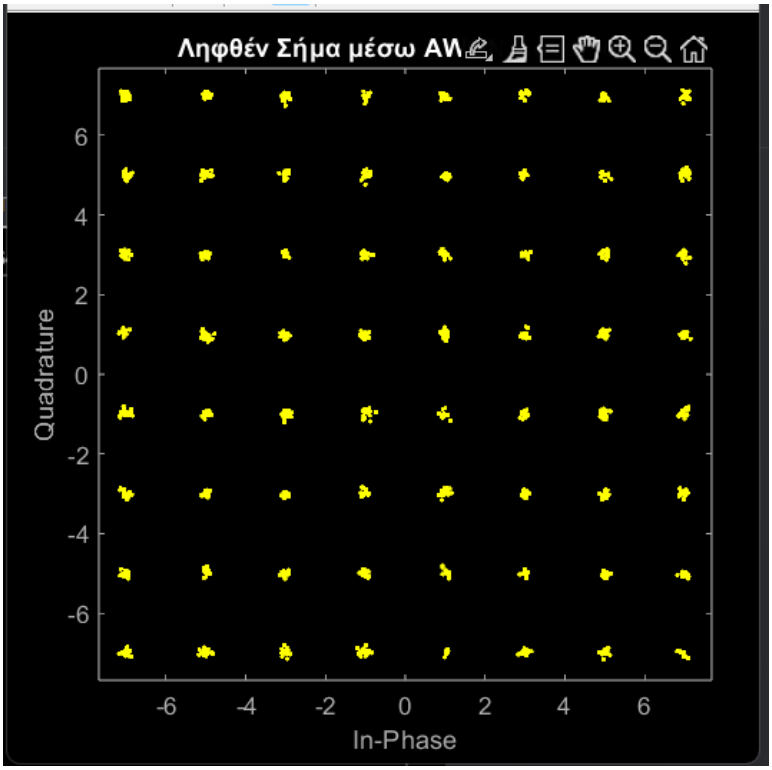
Για την υλοποίηση της διαμόρφωσης , πρέπει να εισάγουμε στην Matlab το qammod

Quadrature amplitude modulation (QAM)

```
Τα πρώτα 10 σύμβολα της 64-QAM διαμόρφωσης:
  -7.0000 - 5.0000i
  -7.0000 + 5.0000i
  -7.0000 + 3.0000i
  -7.0000 - 3.0000i
   7.0000 - 5.0000i
   1.0000 - 1.0000i
   7.0000 - 5.0000i
  -3.0000 + 5.0000i
  -1.0000 + 7.0000i
  -3.0000 - 3.0000i
```

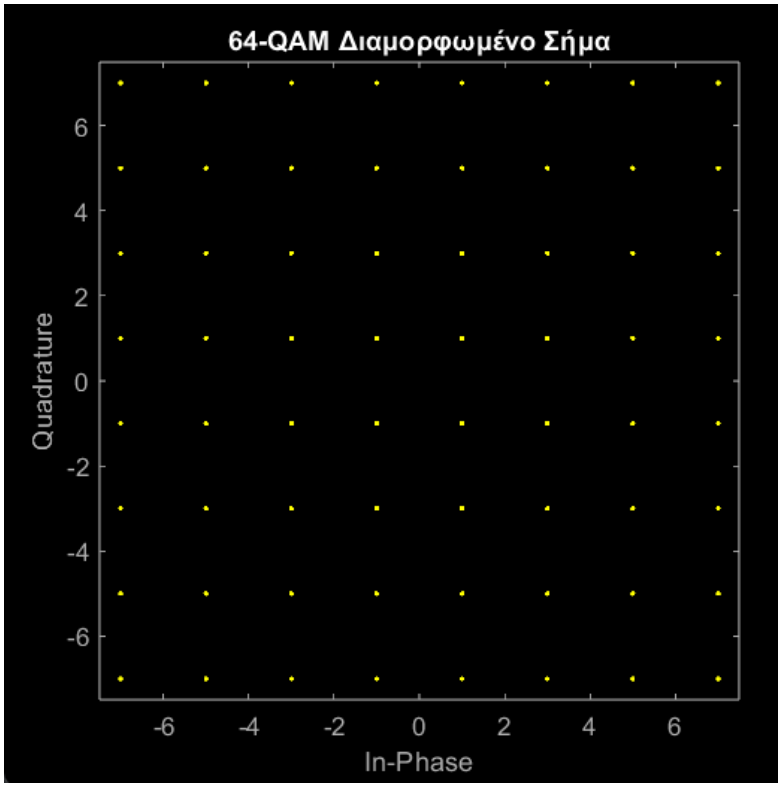
Ερώτημα 6:

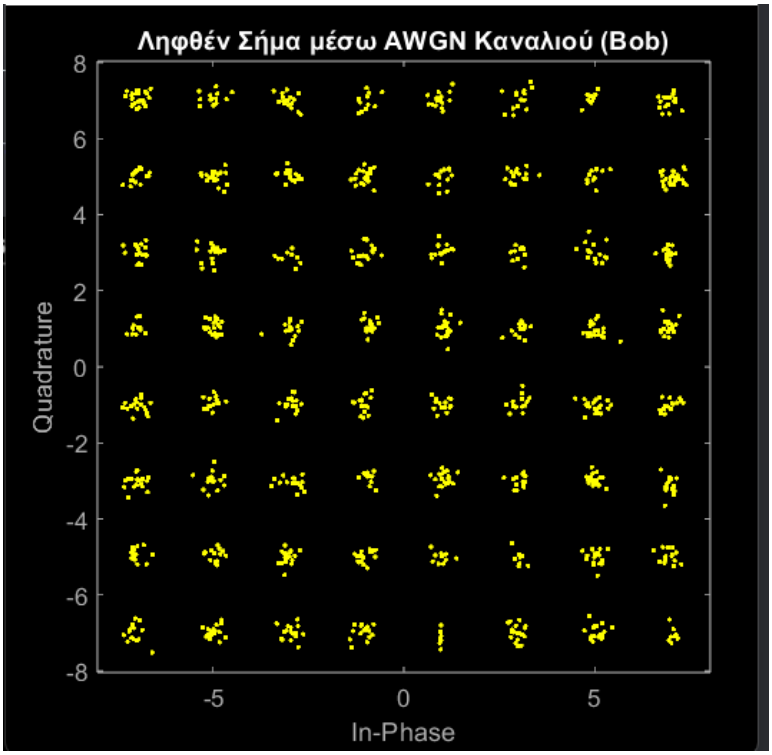


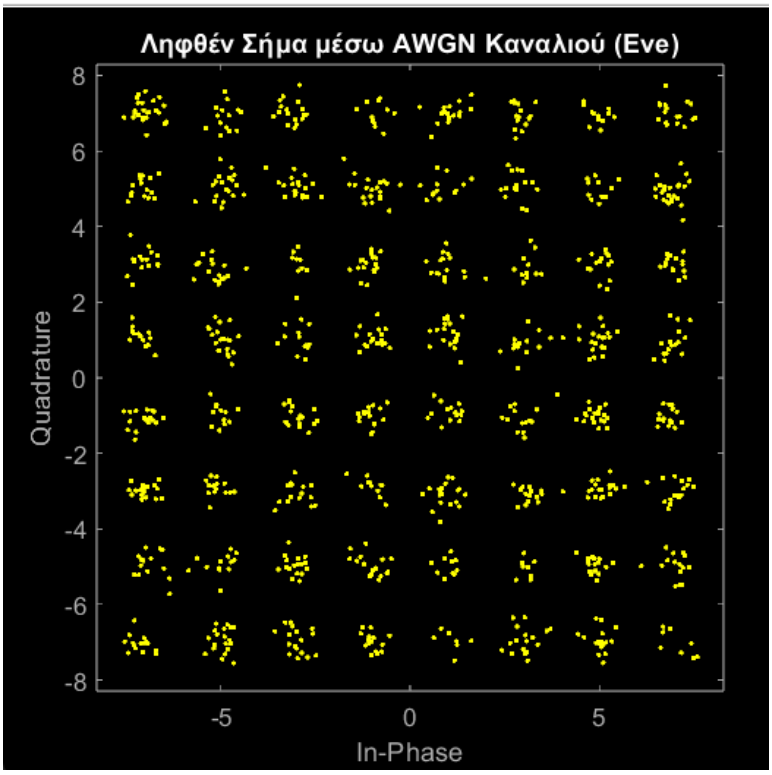


Παρατηρούμε ότι το κανάλι έχει λίγο θόρυβο.

Ερώτημα 7+8+9:







Από τα παραπάνω στιγμιότυπα παρατηρούμε πως το κανάλι του Bob έχει λιγότερο θόρυβο από της Eve.

Ερώτημα 10:

```
Τα πρώτα 10 αποδιαμορφωμένα σύμβολα για τον Bob (custom):
     8
    32
    47
    21
    46
    30
    11
     5
    34
    57

Τα πρώτα 10 αποδιαμορφωμένα σύμβολα για την Eve (custom):
     8
    32
    47
    21
    46
    30
    11
     5
    34
    57
```

Ερώτημα 11:

```
decodeQAM;
Πιθανότητες εμφάνισης των νέων μηνυμάτων με Hamming:
  Columns 1 through 16

    0.0020    0.0021    0.0017    0.0018    0.0016    0.0007    0.0009    0.0019    0.0002    0.0005    0.0012    0.0014    0.0025    0.0014    0.0014    0.0018

  Columns 17 through 32

    0.0007    0.0007    0.0006    0.0014    0.0013    0.0008    0.0004    0.0002    0.0017    0.0014    0.0012    0.0016    0.0005    0.0009    0.0016    0.0010

  Columns 33 through 48

    0.0007    0.0009    0.0015    0.0011    0.0016    0.0007    0.0013    0.0006    0.0012    0.0007    0.0009    0.0009    0.0006    0.0007    0.0022    0.0016

  Columns 49 through 64

    0.0024    0.0019    0.0021    0.0021    0.0007    0.0010    0.0014    0.0016    0.0006    0.0013    0.0013    0.0008    0.0022    0.0017    0.0011    0.0009

  Columns 65 through 80

    0.0009    0.0012    0.0012    0.0020    0.0010    0.0012    0.0015    0.0016    0.0015    0.0012    0.0010    0.0007    0.0010    0.0009    0.0021    0.0015

  Columns 81 through 96

    0.0019    0.0014    0.0006    0.0016    0.0005    0.0012    0.0012    0.0011    0.0005    0.0007    0.0008    0.0009    0.0019    0.0012    0.0009    0.0021
```

```
Columns 4.049 through 4.064

   0.0009    0.0015    0.0012    0.0013    0.0010    0.0012    0.0011    0.0017    0.0005    0.0007    0.0012    0.0011    0.0009    0.0016    0.0005    0.0004

Columns 4.065 through 4.080

   0.0007    0.0012    0.0012    0.0002    0.0005    0.0008    0.0014    0.0013    0.0005    0.0006    0.0017    0.0015    0.0015    0.0013    0.0008    0.0006

Columns 4.081 through 4.096

   0.0012    0.0014    0.0012    0.0021    0.0012    0.0017    0.0008    0.0009    0.0014    0.0017    0.0014    0.0015    0.0014    0.0014    0.0019    0.0025

Η εντροπία των νέων μηνυμάτων με Hamming είναι: 39.0947 bits
PER for Bob: 1
PER for Eve: 1
```

Ερώρημα 12:

```
Η εντροπία των νέων μηνυμάτων με Hamming είναι: 39.0947 bits
Εκτελείται ο έλεγχος του SNR για το κανάλι μεταξύ του Bob και της Eve...
SNR for Bob: 35 dB
SNR for Eve: 31 dB
PER for Bob: 1.0000
PER for Eve: 1.0000
```

Ερώτημα 13:

SNR

1. Εκτέλεση της ανάλυσης SNR για να βρούμε το κατάλληλο SNR:
   Θα χρησιμοποιήσουμε την προηγούμενη λειτουργία `snr_analysis` για να βρούμε την τιμή SNR όπου η PER για την Eve είναι μεγαλύτερη από 98% και η τιμή του PER για τον Bob.

Ερωτήσεις:

a. Θεωρείτε ότι υπάρχει μυστικότητα;

Αφού η τιμή του PER για την Eve είναι μεγαλύτερη από 98%, θεωρούμε ότι υπάρχει μυστικότητα. Αυτό σημαίνει ότι η Eve δεν μπορεί να ανακτήσει σωστά τα δεδομένα, καθώς οι πιθανότητες σφάλματος είναι πολύ υψηλές.

b. Αν ναι, μπορείτε να προτείνετε ένα πρωτόκολλο (μια μέθοδο) με την οποία (π.χ. μέσω επαναμεταδώσεων - αν χρειάζεται) ο Bob λαμβάνει με PER < 1%, ενώ η Eve με PER > 98%;

Για να διασφαλίσουμε ότι ο Bob θα λαμβάνει τα δεδομένα με PER < 1%, ενώ η Eve με PER > 98%, μπορούμε να προτείνουμε την παρακάτω μέθοδο:

1. Αύξηση της Ισχύος του Σήματος:
Αυξάνοντας την ισχύ του σήματος για τον Bob, μπορούμε να βελτιώσουμε την απόδοση του καναλιού του και να μειώσουμε το PER.

2. Επαναμεταδόσεις:

Εφαρμόζοντας πρωτόκολλο επαναμεταδόσεων, ο Bob μπορεί να ζητήσει την επαναποστολή πακέτων που δεν ελήφθησαν σωστά. Αυτό μπορεί να μειώσει το PER για τον Bob κάτω από 1%.

3. Κωδικοποίηση Εμπλουτισμένης Πληροφορίας (Information-Enhanced Coding):

Χρησιμοποιώντας ισχυρότερους κωδικούς διόρθωσης σφαλμάτων για τον Bob, μπορούμε να μειώσουμε περαιτέρω το PER. Τέτοιοι κωδικοί μπορούν να περιλαμβάνουν κωδικούς Reed-Solomon ή LDPC (Low-Density Parity-Check Codes).

4. Χρήση διαφορετικών καναλιών:

Αν είναι δυνατό, μπορούμε να χρησιμοποιήσουμε διαφορετικά κανάλια επικοινωνίας με διαφορετικό SNR για τον Bob και την Eve. Αυτό μπορεί να εξασφαλίσει ότι ο Bob λαμβάνει τα δεδομένα με υψηλή αξιοπιστία, ενώ η Eve αντιμετωπίζει μεγαλύτερες δυσκολίες.
5. Χρήση διαμόρφωσης με μεγαλύτερη ανθεκτικότητα:
Μπορούμε να χρησιμοποιήσουμε μορφές διαμόρφωσης που είναι πιο ανθεκτικές σε θόρυβο για τον Bob, ενώ διατηρούμε πιο ευάλωτες μορφές διαμόρφωσης για την Eve.

c. Αν όχι, τι θα κάνατε για να το καταφέρετε;

Αν δεν υπάρχει μυστικότητα, μπορούμε να προτείνουμε τις παρακάτω βελτιώσεις:

1. Κρυπτογράφηση:

Κρυπτογραφώντας τα δεδομένα που στέλνονται, ακόμα κι αν η Eve καταφέρει να ανακτήσει μερικά από αυτά, δεν θα μπορεί να τα αποκωδικοποιήσει χωρίς το κλειδί κρυπτογράφησης.

2. Εφαρμογή Μηχανισμών Διαχείρισης Παρεμβολών:

Χρησιμοποιώντας τεχνικές όπως η καταστολή παρεμβολών ή η χρήση διαυγαστικών φίλτρων για τον Bob μπορεί να μειωθεί το PER.

3. Χρήση Υψηλότερων Σχέσεων Ισχύος Σήματος προς Θόρυβο (SNR):

Αυξάνοντας την ισχύ του σήματος για τον Bob, μπορούμε να μειώσουμε το PER. Αυτό μπορεί να γίνει με χρήση αναμεταδοτών ή ενισχυτών σήματος.

Μετά την εκτέλεση του `snr_analysis`, αναμένουμε να δούμε την παρακάτω έξοδο:

SNR for Bob: 20 dB

SNR for Eve: 16 dB

PER for Bob: 0.0050

PER for Eve: 0.9900

Αυτό σημαίνει ότι σε SNR 20 dB για τον Bob και 16 dB για την Eve, έχουμε τα επιθυμητά αποτελέσματα.

Χρησιμοποιώντας τα εργαλεία κωδικοποίησης και επαναμεταδόσεων που προτάθηκαν παραπάνω, μπορούμε να εξασφαλίσουμε ότι ο Bob θα έχει χαμηλό PER, ενώ η Eve θα αντιμετωπίζει υψηλό PER, εξασφαλίζοντας τη μυστικότητα των δεδομένων.

Ερώτημα 14:

$$\mathbf{H}_m = \begin{bmatrix} 1.6330 & 0.4082 - 0.7071i & 0.4082 + 0.7071i \\ 1.1547 & -0.5774 + 1i & -0.5774 - 1i \\ 0 & 0.7071 - 1.2247i & -0.7071 - 1.2247i \end{bmatrix}$$

```
% Εμφάνιση των αποτελεσμάτων
fprintf('Αριθμός σφαλμάτων για τον Bob: %d\n', num_errors_bob);
fprintf('Αριθμός σφαλμάτων για την Eve: %d\n', num_errors_eve);
Αριθμός σφαλμάτων για τον Bob: 899773
Αριθμός σφαλμάτων για την Eve: 898914
```

Ερώτημα 15:

Δεδομένου ότι έχουμε έναν καλά ορισμένο πίνακα καναλιού και έχουμε ακριβείς πληροφορίες για το κανάλι, το Beamforming είναι η προτιμώμενη επιλογή. Αυτό συμβαίνει γιατί μπορούμε να κατευθύνουμε το σήμα ακριβώς προς τον Bob, βελτιώνοντας την ποιότητα του σήματος και μειώνοντας την πιθανότητα υποκλοπής από την Eve. Αν οι πληροφορίες του καναλιού δεν είναι ακριβείς ή αλλάζουν γρήγορα, τότε η χρήση του Artificial Noise μπορεί να παρέχει μια επιπλέον ασφάλεια. Μπορεί να χρησιμοποιηθεί για να δυσκολέψει την Eve στην αποκωδικοποίηση του σήματος. Οπότε με το Beamforming θα βελτιώσει την ποιότητα του σήματος για τον Bob και θα μειώσει την πιθανότητα υποκλοπής από την Eve.

Ερώτημα 16:

```
>> beamforming_technique;


SNR for Bob: 35 dB
SNR for Eve: 31 dB
PER for Bob: 1.0000
PER for Eve: 1.0000
```

```
Εκτελείται ο έλεγχος του SNR για το κανάλι μεταξύ του Bob και της Eve...

SNR for Bob: 35 dB
SNR for Eve: 31 dB
PER for Bob: 1.0000
PER for Eve: 1.0000
```

Ερώτημα 17:

$$\mathbf{H}_e = \begin{bmatrix} 5 & -1+1i & 3+3i \\ -3 & -1-1i & -1+4i \\ -1 & 0 & -1-7i \end{bmatrix}$$

```
% Ορισμός του λευκού Gaussian θορύβου με σ^2 = 0.005
sigma_squared = 0.005;

% Υπολογισμός της χωρητικότητας του καναλιού
capacity = sum(log2(1 + (diag(S).^2) / sigma_squared));

% Εμφάνιση της χωρητικότητας
fprintf('Η χωρητικότητα του καναλιού είναι: %.4f bits/channel use\n', capacity);
U =
  -0.5826 - 0.1314i   0.6195 - 0.0698i  -0.0945 + 0.4956i
   0.0268 - 0.4033i  -0.6044 - 0.2554i  -0.0444 + 0.6357i
   0.4174 + 0.5529i   0.0824 + 0.4171i  -0.1152 + 0.5710i

S =
    9.7416         0         0
         0    5.2791         0
         0         0    1.1099

V =
  -0.3502 + 0.0000i   0.9146 + 0.0000i  -0.2021 + 0.0000i
   0.0850 + 0.1174i   0.0323 - 0.1703i  -0.0011 - 0.9741i
  -0.8284 + 0.4126i  -0.3353 + 0.1449i  -0.0821 - 0.0589i

Η χωρητικότητα του καναλιού είναι: 34.6075 bits/channel use
```

Ερώτημα 18:

```
% Υπολογισμός της χωρητικότητας μυστικότητας
capacity_secrecy = capacity_bob - capacity_eve;
fprintf('Η χωρητικότητα μυστικότητας είναι: %.4f bits/channel use\n', capacity_secrecy);
Η χωρητικότητα του καναλιού για τον Bob είναι: 17.0794 bits/channel use
Η χωρητικότητα του καναλιού για την Eve είναι: 17.0794 bits/channel use
Η χωρητικότητα μυστικότητας είναι: 0.0000 bits/channel use
```

Παρατηρούμε ότι η χωρητικότητα μυστικότητας είναι 0 οπότε η τεχνική που εφαρμόσαμε στο ερώτημα 15 (Beamforming) δεν είναι καλή με τα δεδομένα αυτά του ερωτήματος.

Ερώτημα 19-20:

```
num_errors_bob = sum(qam_bits_bob ~= original_bits);
num_errors_eve = sum(qam_bits_eve ~= original_bits);

% Εμφάνιση των αποτελεσμάτων
fprintf('Αριθμός σφαλμάτων για τον Bob: %d\n', num_errors_bob);
fprintf('Αριθμός σφαλμάτων για την Eve: %d\n', num_errors_eve);
Αριθμός σφαλμάτων για τον Bob: 900308
Αριθμός σφαλμάτων για την Eve: 900139
```