



Yalova Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Ana Bilim Dalı

Gömülü Sistem Tasarımı Dersi

Sevdanur GENC - 135105008

Gomulu Sistem Tasarimi

Arduino ile Kriptoloji Uygulamasi

Arduino Nedir



Arduino temel olarak açık kaynaklı bir geliştirme platformuna sahip çevresiyle etkileşimli çalışabilen sistemler tasarlayabileceğiniz bir fiziksel programlama platformudur.

Arduino kartları üzerinde Atmega firmasına ait 8 ve 32 bitlik mikrodenetleyiciler bulunmakla birlikte analog ve digital girişleri sayesinde de analog ve digital verilerle de çalışılabilir. Arduino IDE kod editörü ve derleyicisi sayesinde derlenen programı Arduino kartlarına yükleyebilirsiniz, her platformda çalışabilecek Java programlama dilinde yazılmış bir uygulamadır.

Arduino IDE'ye, Library ve Example kodlara resmi sitesi arduino.cc 'den ulaşabilirsiniz.

Genel anlamda Arduino'nun sahip olduğu özellikler;

Atmega328 mikrodenetleyici

USB ve adaptor bağlantı portları

Güç regülatörü

3.3V veya 5V çalışma gerilimi

14 dijital ve 6 analog giriş/çıkış

16kb Flash bellek

3.3V için 8Mhz ve 5V için 16Mhz çalışma hızı



Arduino Uno R3 Front & Back

Kriptoloji Uygulaması

Kullanici tarafından girilen metinlerin nukleotid bazlarına donusturulmesi ya da girilen nukleotid dizilimlerinin metine donusturulmesini saglayan ve arduino uzerinde calisan bir sifreleme programidir.

Ornek verilecek olursa;

Nukleotid Dizilimi	Metin Karsiligi
AAGTATAGTGCATTATTGACCGAGGACGCTAACTGGTCAT	DENEYLER
AGCTGAGGCACAATCGATTTACCGTTATTAAGCGGATATT	KLONLAMA

Kurallar : Alfabedeki her bir buyuk harfin 5 bit'lik kodlamasi gerceklestirilir.

00000	A	0	00110	F	6	01100	J	12	10010	Ö	18	11000	U	24
00001	B	1	00111	G	7	01101	K	13	10011	O	19	11001	Ü	25
00010	C	2	01000	G	8	01110	L	14	10100	R	20	11010	V	26
00011	Ç	3	01001	H	9	01111	M	15	10101	S	21	11011	Y	27
00100	D	4	01010	I	10	10000	N	16	10110	S	22	11100	Z	28
00101	E	5	01011	I	11	10001	O	17	10111	T	23			

Ardindan, 0 bit'in esitligi "A" veya "T" nukleotid bazlarindan rastgele, 1 bit'in esitligi "G" veya "C" nukleotid bazlarindan rastgele secim yapilmis olacak.

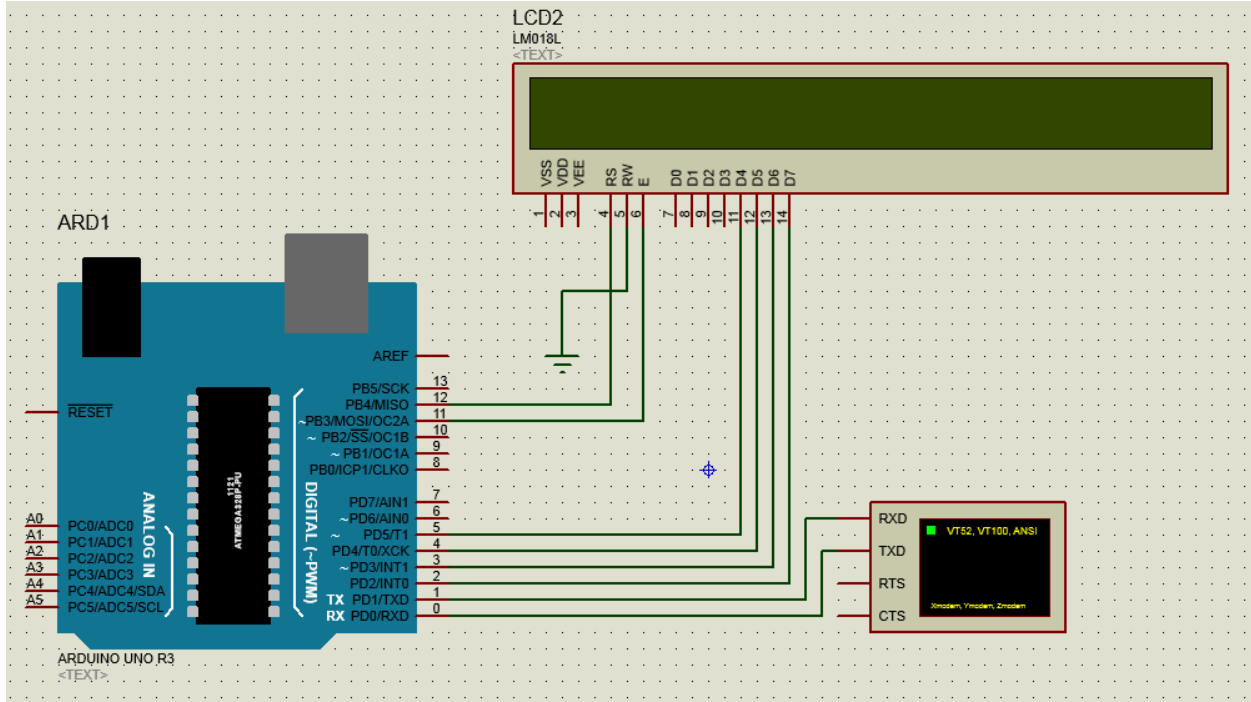
Ornegin; AGCTGAGGCACAATCGATTTACCGTTATTAAGCGGATATT dizisi 5'er gruplara ayrilip bit'e donusturulduygunde, ondalik degerleri ile birlikte harf degerleride cozumlenmis olacak.

AGCTG: bit deęeri: 01101, ondalık deęeri: 13, harf: K
 AGGCA: bit deęeri: 01110, ondalık deęeri: 14, harf: L
 CAATC: bit deęeri: 10001, ondalık deęeri: 17, harf: O
 GATTT: bit deęeri: 10000, ondalık deęeri: 16, harf: N
 ACCGT: bit deęeri: 01110, ondalık deęeri: 14, harf: L
 TATTA: bit deęeri: 00000, ondalık deęeri: 0, harf: A
 AGCGG: bit deęeri: 01111, ondalık deęeri: 15, harf: M
 ATATT: bit deęeri: 00000, ondalık deęeri: 0, harf: A

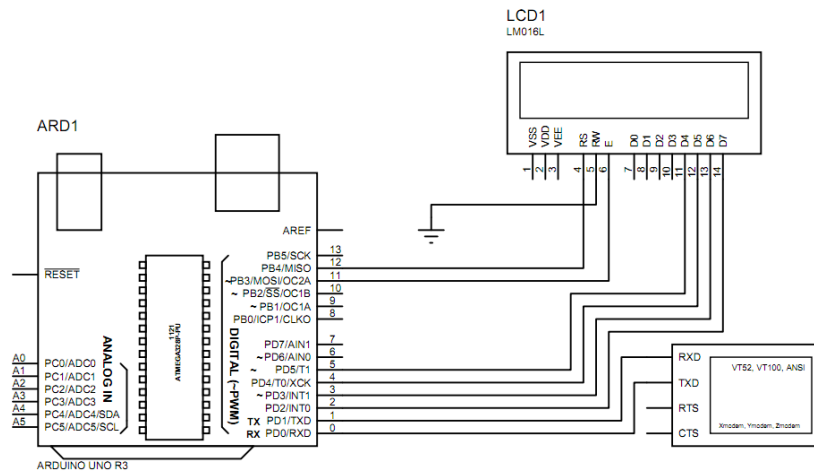
Referans: Tubitak - Bilgem, Subat Ayi Odullu Sorulari, Soru 1 http://bilgem.tubitak.gov.tr/sites/images/2012_subat_soru_cevap.pdf

Proteus Tasarimi

Devices : Arduino Uno R3, LM018L - LCD display, Virtual Terminal, Ground



LCD RS pin'i Arduino digital pin 12'ye
 LCD Enable pin'i Arduino digital pin 11'e
 LCD D4 pin'i Arduino digital pin 5'e
 LCD D5 pin'i Arduino digital pin 4'e
 LCD D6 pin'i Arduino digital pin 3'e
 LCD D7 pin'i Arduino digital pin 2'ye
 Virtual Terminal RXD pin'i Arduino digital pin 1'e
 Virtual Terminal TXD pin'i Arduino digital pin 0'a
 LCD RW pin'i GND'ye baglariz.



Arduino Kod Tasarimi

```
#include <LiquidCrystal.h>
LiquidCrystal lcd(12, 11, 5, 4, 3, 2);
String harf, yeniKelime, bitDonustur, harfDonustur, al, hecele;
int temp, count = 0;
char oku[100];

void setup() {
  Serial.begin(9600);
  //DNA("AAGTATAGTGCATTATTGACCGAGGACGCTAACTGGTCAT");
  //DNA("AGCTGAGGCACAATCGATTTACCGTTATTAAGCGGATATT");
  Serial.println("Kriptoloji Yonteminiz...");
}

void loop() {
  if (Serial.available() > 0)
  {
    oku[count] = (char)Serial.read();
    if (oku[count++] == '\r')
    {
      oku[count] = '\0';
      //Serial.println("1 . Metin ---> DNA"); Serial.print(oku); lcd.clear(); MetintoDNA(oku);
      Serial.println("2 . DNA ---> Metin"); Serial.print(oku); lcd.clear(); DNAtoMetin(oku);
      count = 0;
    }
  }
}

void DNAtoMetin(String sequence)
{
  for (int i=0; i<sequence.length(); i +=5)
  {
    bitDonustur = donustur(sequence.substring(i, i+5));
    harfDonustur = cozumle(yeniKelime);
    lcd.print(harfDonustur);
  }
}

void MetintoDNA(String sequence)
{
  for (int i=0; i<sequence.length(); i++)
  {
    harfDonustur = butunlestir(sequence.substring(i,i+1));
    bitDonustur = olustur(harfDonustur);
    lcd.print(bitDonustur);
  }
}
```

```

    }
}

```

String donustur(String kelime)

```

{
    yeniKelime = "";
    for (int i=0; i<kelime.length(); i++)
    {
        if (kelime.charAt(i) == 'A' || kelime.charAt(i) == 'T') temp=0;
        if (kelime.charAt(i) == 'G' || kelime.charAt(i) == 'C') temp=1;
        yeniKelime = yeniKelime + temp;
    }
    return yeniKelime;
}

```

String cozumle(String hecele)

```

{
    if (hecele.equals("00000")) harf = "A"; //0
    if (hecele.equals("00001")) harf = "B"; //1
    if (hecele.equals("00010")) harf = "C"; //2
    if (hecele.equals("00011")) harf = "Ç"; //3
    if (hecele.equals("00100")) harf = "D"; //4
    if (hecele.equals("00101")) harf = "E"; //5
    if (hecele.equals("00110")) harf = "F"; //6
    if (hecele.equals("00111")) harf = "G"; //7
    if (hecele.equals("01000")) harf = "G"; //8
    if (hecele.equals("01001")) harf = "H"; //9
    if (hecele.equals("01010")) harf = "I"; //10
    if (hecele.equals("01011")) harf = "I"; //11
    if (hecele.equals("01100")) harf = "J"; //12
    if (hecele.equals("01101")) harf = "K"; //13
    if (hecele.equals("01110")) harf = "L"; //14
    if (hecele.equals("01111")) harf = "M"; //15
    if (hecele.equals("10000")) harf = "N"; //16
    if (hecele.equals("10001")) harf = "O"; //17
    if (hecele.equals("10010")) harf = "Ö"; //18
    if (hecele.equals("10011")) harf = "P"; //19
    if (hecele.equals("10100")) harf = "R"; //20
    if (hecele.equals("10101")) harf = "S"; //21
    if (hecele.equals("10110")) harf = "S"; //22
    if (hecele.equals("10111")) harf = "T"; //23
    if (hecele.equals("11000")) harf = "U"; //24
    if (hecele.equals("11001")) harf = "Ü"; //25
    if (hecele.equals("11010")) harf = "V"; //26
    if (hecele.equals("11011")) harf = "Y"; //27
    if (hecele.equals("11100")) harf = "Z"; //28
}

```

```

    return harf;
}

String olustur(String kelime)
{
    yeniKelime = "";
    //Random rnd = new Random();
    for (int i=0; i<kelime.length(); i++)
    {
        if (kelime.charAt(i) == '0'){
            temp = random(2);
            if (temp == 0) al = "A";
            if (temp == 1) al = "T";
        }
        if (kelime.charAt(i) == '1'){
            temp = random(2);
            if (temp == 0) al = "G";
            if (temp == 1) al = "C";
        }
        yeniKelime = yeniKelime + al;
    }
    return yeniKelime;
}

```

```

String butunlestir(String harf)
{
    if (harf.equals("A")) hecele = "00000"; //0
    if (harf.equals("B")) hecele = "00001"; //1
    if (harf.equals("C")) hecele = "00010"; //2
    if (harf.equals("Ç")) hecele = "00011"; //3
    if (harf.equals("D")) hecele = "00100"; //4
    if (harf.equals("E")) hecele = "00101"; //5
    if (harf.equals("F")) hecele = "00110"; //6
    if (harf.equals("G")) hecele = "00111"; //7
    if (harf.equals("G")) hecele = "01000"; //8
    if (harf.equals("H")) hecele = "01001"; //9
    if (harf.equals("I")) hecele = "01010"; //10
    if (harf.equals("I")) hecele = "01011"; //11
    if (harf.equals("J")) hecele = "01100"; //12
    if (harf.equals("K")) hecele = "01101"; //13
    if (harf.equals("L")) hecele = "01110"; //14
    if (harf.equals("M")) hecele = "01111"; //15
    if (harf.equals("N")) hecele = "10000"; //16
    if (harf.equals("O")) hecele = "10001"; //17
    if (harf.equals("Ö")) hecele = "10010"; //18
    if (harf.equals("P")) hecele = "10011"; //19
}

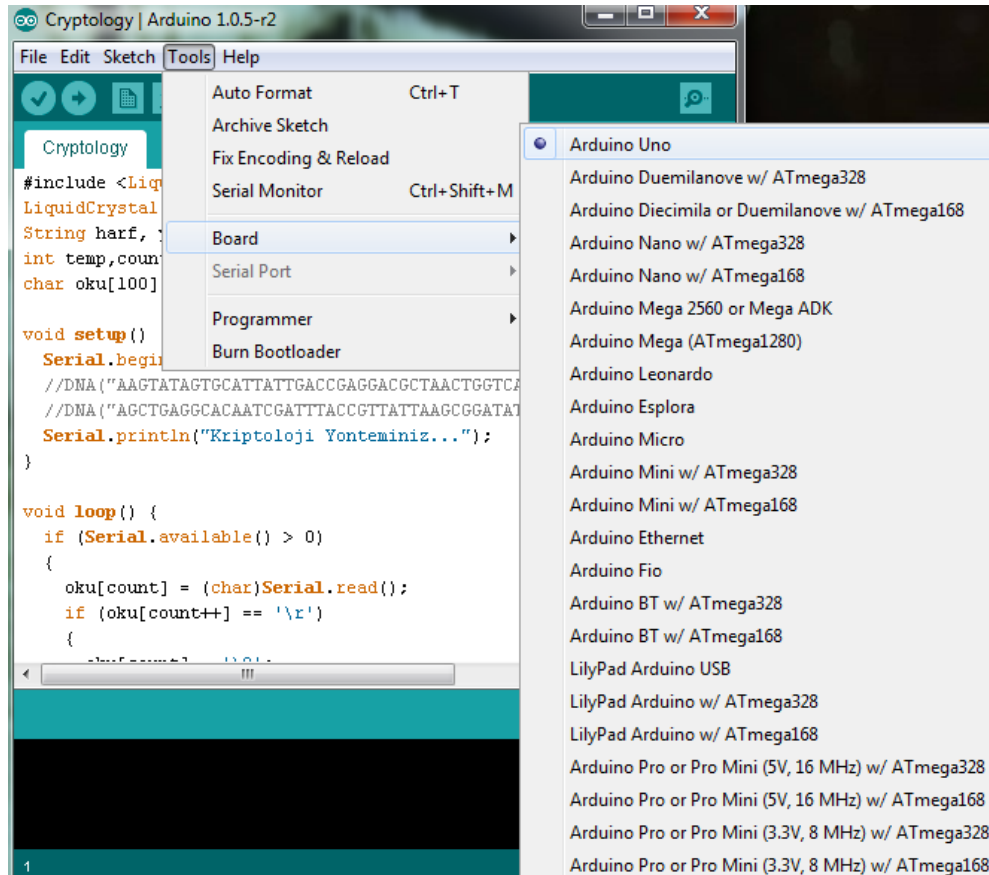
```

```

if (harf.equals("R")) hecele = "10100"; //20
if (harf.equals("S")) hecele = "10101"; //21
if (harf.equals("S")) hecele = "10110"; //22
if (harf.equals("T")) hecele = "10111"; //23
if (harf.equals("U")) hecele = "11000"; //24
if (harf.equals("Ü")) hecele = "11001"; //25
if (harf.equals("V")) hecele = "11010"; //26
if (harf.equals("Y")) hecele = "11011"; //27
if (harf.equals("Z")) hecele = "11100"; //28
return hecele;
}

```

Kodlama yapıldıktan sonra proteus üzerinde hangi arduino kullaniliyorsa ayni sekilde kodu derleme yaparken tool menusunen board'ini da benzer secmeliyiz. Proteus tasariminda Arduino Uno R3 kullandigim icin kodumu compile ederken Board'u Arduino Uno'yu seciyorum.



Compile edilen koda ait hex dosyasini proteus'ta ki arduino'ya gomdukten sonra asagidaki ekran görüntülerine ait sonuclari elde etmis oluyorum.

Uygulama Sonuclari

