# DNA Computing Based Encryption & Decryption Algorithm

ICT 4011 Natural Computing

Dept of Information and Communication Technology
Manipal Institute of Technology
Manipal -576104

# Requirement of DNA Encryption Algorithm

1. DNA Encoding of complete character set
2. Dynamic Encoding Table Generation
3. Unique sequence for encoding of every character of plaintext to DNA sequence
4. Robustness of Encoding
5. Biological Process Simulation
6. Dynamicity of Encryption Process

# DNA Encryption-Decryption Algorithm

1. DNA Computing based Encoding Algorithm
2. DNA Computing based Encryption & Decryption Algorithm

# DNA Encoding Table

| | C | A | T | G |
|---|---|---|---|---|
| A | ACAT- a | AAAA – y | ATAA– W | AGAG – { |
| | ACTG- b | AATT – z | ATTT – X | AGTA – [ |
| | ACCC- c | AACC – A | ATCG – Y | AGCG - } |
| | ACGA – d | AAGG– B | ATGC – Z | AGGG - ] |
| T | TCAT – e | TAAT – C | TTAA – 0 | TGAA - \| |
| | TCTG – f | TATG – D | TTTT – 1 | TGTT - \ |
| | TCCG – g | TACC – E | TTCC – 2 | TGCG - + |
| | TCGT – h | TAGA – F | TTGG - 3 | TGGC - = |
| C | CCAG – i | CAAT – G | CTAT – 4 | CGAA - _ |
| | CCTA – j | CATG – H | CTTG – 5 | CGTT - - |
| | CCCG – k | CACG – I | CTCC – 6 | CGCC - ) |
| | CCGG – l | CAGT – J | CTGA – 7 | CGGG – ( |
| G | GCAA – m | GAAG– K | GTAT – 8 | GGAT - * |
| | GCTT – n | GATA – L | GTTG – 9 | GGTG - & |
| | GCCG – o | GACG– M | GTCG – < | GGCC - ^ |
| | GCGC – p | GAGG– N | GTGT - > | GGGA - % |
| A | ACTC – q | AATA – O | ATTA - , | AGTT - $ |
| | ACCG – r | AACG – P | ATCC - . | AGCC - # |
| T | TCTC – s | TATC – Q | TTTA - ? | TGTA - @ |
| | TCCC – t | TACG – R | TTCG - / | TGCC - ! |
| C | CCTT – u | CATC – S | CTTC - : | CGTA - ~ |
| | CCCC – v | CACC – T | CTCG - ; | CGCG - ` |
| G | GCTA – w | GATT – U | GTTC – “ | GGTC - € |
| | GCCC – x | GACC – V | GTCC – ‘ | GGCG - £ |

# Encryption Process

1. Generation of encoding table 1 & 2
2. Plaintext converted into DNA sequence (Encoding table1 &2)
3. Multiple round functions are performed: (min 10 rounds)
    a. DNA sequence XNOR with introns
    b. DNA converted to mRNA (transcription process) T -> U
    c. mRNA to tRNA (translation process) complement
    d. tRNA to DNA (reverse transcription) U -> T
    e. Right Shift the sequences
4. tRNA obtained is converted amino acids
5. The resultant protein sequence is the cipher text

# Amino Acid Table

Table.6. Amino acid Table

| | GA | UA | AA | CA | CU | AU | UU | GU | GC | UC | AC | CC | CG | AG | UG | GG |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CG | CGGA | CGUA | CGAA | CGCA | CGCU | CGAU | CGUU | CGGU | CGGC | CGUC | CGAC | CGCC | CGCG | CGAG | CGUG | CGGG |
| | – E1 | – Q4 | – G7 | – HA | – A1 | – R4 | – N7 | – DA | – L1 | – K4 | – M7 | – FA | – S1 | – U4 | – W7 | – YA |
| AG | AGGA | AGUA | AGAA | AGCA | AGCU | AGAU | AGUU | AGGU | AGGC | AGUC | AGAC | AGCC | AGCG | AGAG | AGUG | AGGG |
| | – E2 | – Q5 | – G8 | – HB | – A2 | – R5 | – N8 | – DB | – L2 | – K5 | – M8 | – FB | – S2 | – U5 | – W8 | – YB |
| UG | UGGA | UGUA | UGAA | UGCA | UGCU | UGAU | UGUU | UGGU | UGGC | UGUC | UGAC | UGCC | UGCG | UGAG | UGUG | UGGG |
| | – E3 | – Q6 | – G9 | – HC | – A3 | – R6 | – N9 | – DC | – L3 | – K6 | – M9 | – FC | – S3 | – U6 | – W9 | – YC |
| GG | GGGA | GGUA | GGAA | GGCA | GGCU | GGAU | GGUU | GGGU | GGGC | GGUC | GGAC | GGCC | GGCG | GGAG | GGUG | GGGG |
| | – E4 | – Q7 | – GA | – HD | – A4 | – R7 | – NA | – DD | – L4 | – K7 | – MA | – FD | – S4 | – U7 | – WA | – YD |
| GC | GCGA | GCUA | GCAA | GCCA | GCCU | GCAU | GCUU | GCGU- | GCGC | GCUC | GCAC | GCCC | GCCG | GCAG | GCUG | GCGG |
| | – E5 | – Q8 | – GB | – I1 | – A5 | – R8 | – NB | C1 | – L5 | – K8 | – MB | – P1 | – S5 | - U8 | – WB | – V1 |
| UC | UCGA | UCUA | UCAA | UCCA | UCCU | UCAU | UCUU | UCGU | UCGC | UCUC | UCAC | UCCC | UCCG | UCAG | UCUG | UCGG |
| | – E6 | – Q9 | – GC | – I2 | – A6 | – R9 | – NC | – C2 | – L6 | – K9 | – MC | – P2 | – S6 | – U9 | – WC | – V2 |
| AC | ACGA | ACUA | ACAA | ACCA | ACCU | ACAU | ACUU | ACGU | ACGC | ACUC | ACAC | ACCC- | ACCG | ACAG | ACUG | ACGG |
| | – E7 | – QA | – GD | – I3 | – A7 | – RA | – ND | – C3 | – L7 | – KA | – MD | P3 | – S7 | – UA | – WD | – V3 |
| CC | CCGA | CCUA | CCAA | CCCA | CCCU | CCAU | CCUU | CCGU | CCGC | CCUC | CCAC | CCCC | CCCG | CCAG | CCUG | CCGG |
| | – E8 | – QB | – H1 | – I4 | – A8 | – RB | – D1 | – C4 | – L8 | – KB | – F1 | – P4 | – S8 | - UB | – Y1 | – V4 |
| CU | CUGA | CUUA | CUAA | CUCA | CUCU | CUAU | CUUU | CUGU | CUGC | CUUC | CUAC | CUCC | CUCG | CUAG | CUUG | CUGG |
| | – E9 | – QC | – H2 | – I5 | – A9 | – RC | – D2 | – C5 | – L9 | – KC | – F2 | – P5 | – S9 | – UC | – Y2 | – V5 |
| AU | AUGA | AUUA | AUAA | AUCA | AUCU | AUAU | AUUU– | AUGU | AUGC | AUUC | AUAC | AUCC | AUCG | AUAG | AUUG | AUGG |
| | – EA | – QD | – H3 | – I6 | – AA | – RD | D3 | – C6 | – LA | – KD | – F3 | – P6 | – SA | – UD | – Y3 | – V6 |
| UU | UUGA | UUUA | UUAA | UUCA | UUCU | UUAU | UUUU | UUGU | UUGC | UUUC | UUAC | UUCC | UUCG | UUAG | UUUG | UUGG |
| | – EB | – G1 | – H4 | – I7 | – AB | – N1 | – D4 | – C7 | – LB | – M1 | – F4 | – P7 | – SB | – W1 | – Y4 | – V7 |
| GU | GUGA | GUUA | GUAA | GUCA | GUCU | GUAU | GUUU | GUGU | GUGC | GUUC | GUAC | GUCC | GUCG | GUAG | GUUG | GUGG |
| | – EC | – G2 | – H5 | – I8 | – AC | – N2 | – D5 | – C8 | – LC | – M2 | – F5 | – P8 | – SC | – W2 | – Y5 | – V8 |
| GA | GAGA | GAUA | GAAA | GACA | GACU | GAAU | GAUU | GAGU | GAGC | GAUC | GAAC | GACC | GACG | GAAG | GAUG | GAGG |
| | – ED | – G3 | – H6 | – I9 | – AD | – N3 | – D6 | – C9 | – LD | – M3 | – F6 | – P9 | – SD | – W3 | – Y6 | – V9 |
| UA | UAGA | UAUA | UAAA | UACA | UACU | UAAU | UAUU | UAGU | UAGC | UAUC | UAAC | UACC | UACG | UAAG | UAUG | UAGG |
| | – Q1 | – G4 | – H7 | – IA | – R1 | – N4 | – D7 | – CA | – K1 | – M4 | – F7 | – PA | – U1 | – W4 | - Y7 | – VA |
| AA | AAGA | AAUA | AAAA | AACA | AACU | AAAU | AAUU | AAGU | AAGC | AAUC | AAAC | AACC | AACG | AAAG | AAUG | AAGG |
| | – Q2 | – G5 | – H8 | – IB | – R2 | – N5 | – D8 | – CB | – K2 | – M5 | – F8 | – PB | – U2 | – W5 | – Y8 | – VB |
| CA | CAGA | CAUA | CAAA | CACA | CACU | CAAU- | CAUU | CAGU | CAGC | CAUC | CAAC | CACC | CACG | CAAG | CAUG | CAGG |
| | – Q3 | – G6 | – H9 | – IC | – R3 | N6 | – D9 | – CC | – K3 | – M6 | – F9 | – PC | – U3 | – W6 | – Y9 | – VC |

# Amino-Acid Table Generation

1. Generation of 2 DNA sequences randomly (4 DNA alphabets) Ex: ATCG, GTAC
2. Converting sequences into mRNA
3. Assigning 2 mRNA row-wise and column-wise in 4x4 matrix

Table.4. Amino Acid Table

| A | U | C | G |
|---|---|---|---|
| GA | GU | GC | GG |
| UA | UU | UC | UG |
| AA | AU | AC | AG |
| CA | CU | CC | CG |

4. The 4x4 matrix extended to 16x16
5. Amino acids divided into four groups
6. 24 possible collating sequences , Using any one of the sequence

# Amino-Acid Table Generation

| | GA | UA | AA | CA | CU | AU | UU | GU | GC | UC | AC | CC | CG | AG | UG | GG |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CG** | CGGA | CGUA | CGAA | CGCA | CGCU | CGAU | CGUU | CGGU | CGGC | CGUC | CGAC | CGCC | CGCG | CGAG | CGUG | CGGG |
| **AG** | AGGA | AGUA | AGAA | AGCA | AGCU | AGAU | AGUU | AGGU | AGGC | AGUC | AGAC | AGCC | AGCG | AGAG | AGUG | AGGG |
| **UG** | UGGA | UGUA | UGAA | UGCA | UGCU | UGAU | UGUU | UGGU | UGGC | UGUC | UGAC | UGCC | UGCG | UGAG | UGUG | UGGG |
| **GG** | GGGA | GGUA | GGAA | GGCA | GGCU | GGAU | GGUU | GGGU | GGGC | GGUC | GGAC | GGCC | GGCG | GGAG | GGUG | GGGG |
| **GC** | GCGA | GCUA | GCAA | GCCA | GCCU | GCAU | GCUU | GCGU | GCGC | GCUC | GCAC | GCCC | GCCG | GCAG | GCUG | GCGG |
| **UC** | UCGA | UCUA | UCAA | UCCA | UCCU | UCAU | UCUU | UCGU | UCGC | UCUC | UCAC | UCCC | UCCG | UCAG | UCUG | UCGG |
| **AC** | ACGA | ACUA | ACAA | ACCA | ACCU | ACAU | ACUU | ACGU | ACGC | ACUC | ACAC | ACCC | ACCG | ACAG | ACUG | ACGG |
| **CC** | CCGA | CCUA | CCAA | CCCA | CCCU | CCAU | CCUU | CCGU | CCGC | CCUC | CCAC | CCCC | CCCG | CCAG | CCUG | CCGG |
| **CU** | CUGA | CUUA | CUAA | CUCA | CUCU | CUAU | CUUU | CUGU | CUGC | CUUC | CUAC | CUCC | CUCG | CUAG | CUUG | CUGG |
| **AU** | AUGA | AUUA | AUAA | AUCA | AUCU | AUAU | AUUU | AUGU | AUGC | AUUC | AUAC | AUCC | AUCG | AUAG | AUUG | AUGG |
| **UU** | UUGA | UUUA | UUAA | UUCA | UUCU | UUAU | UUUU | UUGU | UUGC | UUUC | UUAC | UUCC | UUCG | UUAG | UUUG | UUGG |
| **GU** | GUGA | GUUA | GUAA | GUCA | GUCU | GUAU | GUUU | GUGU | GUGC | GUUC | GUAC | GUCC | GUCG | GUAG | GUUG | GUGG |
| **GA** | GAGA | GAUA | GAAA | GACA | GACU | GAAU | GAUU | GAGU | GAGC | GAUC | GAAC | GACC | GACG | GAAG | GAUG | GAGG |
| **UA** | UAGA | UAUA | UAAA | UACA | UACU | UAAU | UAUU | UAGU | UAGC | UAUC | UAAC | UACC | UACG | UAAG | UAUG | UAGG |
| **AA** | AAGA | AAUA | AAAA | AACA | AACU | AAAU | AAUU | AAGU | AAGC | AAUC | AAAC | AACC | AACG | AAAG | AAUG | AAGG |
| **CA** | CAGA | CAUA | CAAA | CACA | CACU | CAAU | CAUU | CAGU | CAGC | CAUC | CAAC | CACC | CACG | CAAG | CAUG | CAGG |

# Amino-Acid Table Generation

**A group** – (A1, A2, A3, A4, A5, A6, A7, A8, A9, AA, AB, AC,AD, R1, R2, R3, R4, R5, R6, R7, R8, R9, RA, RB, RC,RD, N1,N2, N3, N4, N5, N6, N7, N8, N9, NA, NB, NC, ND, D1,D2,D3,D4,D5,D6,D7, D8, D9, DA, DB, DC, DD, C1, C2, C3, C4, C5, C6, C7, C8, C9, CA,CB,CC )

**U group** – (E1, E2, E3, E4, E5, E6, E7, E8, E9, EA, EB, EC,ED, Q1, Q2, Q3, Q4, Q5, Q6, Q7, Q8, Q9, QA, QB, QC, QD, G1, G2, G3, G4, G5, G6, G7, G8, G9, GA, GB, GC, GD, H1, H2, H3, H4, H5, H6, H7, H8, H9, HA, HB, HC, HD, I1, I2, I3, I4, I5, I6, I7, I8, I9, IA, IB, IC)

**C group** – (L1, L2, L3, L4, L5, L6, L7, L8, L9, LA, LB, LC,LD,K1, K2, K3, K4, K5, K6, K7, K8, K9, KA, KB, KC, KD, M1, M2, M3, M4, M5, M6, M7, M8, M9, MA, MB, MC,MD,F1, F2, F3, F4, F5, F6, F7, F8, F9, FA, FB, FC, FD, P1, P2, P3, P4, P5, P6, P7, P8, P9, PA, PB, PC)

**G group** – (S1, S2, S3, S4, S5, S6, S7, S8, S9, SA, SB, SC, SD, T1, T2, T3, T4, T5, T6, T7, T8, T9, TA, TB, TC, TD, W1, W2, W3, W4, W5, W6, W7, W8, W9, WA, WB, WC,WD, Y1,Y2, Y3, Y4, Y5, Y6, Y7, Y8, Y9, YA, YB, YC,YD,V1,V2, V3, V4, V5, V6, V7, V8, V9, VA, VB, VC)

# Amino Acid Table

Table.6. Amino acid Table

| | GA | UA | AA | CA | CU | AU | UU | GU | GC | UC | AC | CC | CG | AG | UG | GG |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CG | CGGA | CGUA | CGAA | CGCA | CGCU | CGAU | CGUU | CGGU | CGGC | CGUC | CGAC | CGCC | CGCG | CGAG | CGUG | CGGG |
| | – E1 | – Q4 | – G7 | – HA | – A1 | – R4 | – N7 | – DA | – L1 | – K4 | – M7 | – FA | – S1 | – U4 | – W7 | – YA |
| AG | AGGA | AGUA | AGAA | AGCA | AGCU | AGAU | AGUU | AGGU | AGGC | AGUC | AGAC | AGCC | AGCG | AGAG | AGUG | AGGG |
| | – E2 | – Q5 | – G8 | – HB | – A2 | – R5 | – N8 | – DB | – L2 | – K5 | – M8 | – FB | – S2 | – U5 | – W8 | – YB |
| UG | UGGA | UGUA | UGAA | UGCA | UGCU | UGAU | UGUU | UGGU | UGGC | UGUC | UGAC | UGCC | UGCG | UGAG | UGUG | UGGG |
| | – E3 | – Q6 | – G9 | – HC | – A3 | – R6 | – N9 | – DC | – L3 | – K6 | – M9 | – FC | – S3 | – U6 | – W9 | – YC |
| GG | GGGA | GGUA | GGAA | GGCA | GGCU | GGAU | GGUU | GGGU | GGGC | GGUC | GGAC | GGCC | GGCG | GGAG | GGUG | GGGG |
| | – E4 | – Q7 | – GA | – HD | – A4 | – R7 | – NA | – DD | – L4 | – K7 | – MA | – FD | – S4 | – U7 | – WA | – YD |
| GC | GCGA | GCUA | GCAA | GCCA | GCCU | GCAU | GCUU | GCGU- | GCGC | GCUC | GCAC | GCCC | GCCG | GCAG | GCUG | GCGG |
| | – E5 | – Q8 | – GB | – I1 | – A5 | – R8 | – NB | C1 | – L5 | – K8 | – MB | – P1 | – S5 | - U8 | – WB | – V1 |
| UC | UCGA | UCUA | UCAA | UCCA | UCCU | UCAU | UCUU | UCGU | UCGC | UCUC | UCAC | UCCC | UCCG | UCAG | UCUG | UCGG |
| | – E6 | – Q9 | – GC | – I2 | – A6 | – R9 | – NC | – C2 | – L6 | – K9 | – MC | – P2 | – S6 | – U9 | – WC | – V2 |
| AC | ACGA | ACUA | ACAA | ACCA | ACCU | ACAU | ACUU | ACGU | ACGC | ACUC | ACAC | ACCC- | ACCG | ACAG | ACUG | ACGG |
| | – E7 | – QA | – GD | – I3 | – A7 | – RA | – ND | – C3 | – L7 | – KA | – MD | P3 | – S7 | – UA | – WD | – V3 |
| CC | CCGA | CCUA | CCAA | CCCA | CCCU | CCAU | CCUU | CCGU | CCGC | CCUC | CCAC | CCCC | CCCG | CCAG | CCUG | CCGG |
| | – E8 | – QB | – H1 | – I4 | – A8 | – RB | – D1 | – C4 | – L8 | – KB | – F1 | – P4 | – S8 | - UB | – Y1 | – V4 |
| CU | CUGA | CUUA | CUAA | CUCA | CUCU | CUAU | CUUU | CUGU | CUGC | CUUC | CUAC | CUCC | CUCG | CUAG | CUUG | CUGG |
| | – E9 | – QC | – H2 | – I5 | – A9 | – RC | – D2 | – C5 | – L9 | – KC | – F2 | – P5 | – S9 | – UC | – Y2 | – V5 |
| AU | AUGA | AUUA | AUAA | AUCA | AUCU | AUAU | AUUU– | AUGU | AUGC | AUUC | AUAC | AUCC | AUCG | AUAG | AUUG | AUGG |
| | – EA | – QD | – H3 | – I6 | – AA | – RD | D3 | – C6 | – LA | – KD | – F3 | – P6 | – SA | – UD | – Y3 | – V6 |
| UU | UUGA | UUUA | UUAA | UUCA | UUCU | UUAU | UUUU | UUGU | UUGC | UUUC | UUAC | UUCC | UUCG | UUAG | UUUG | UUGG |
| | – EB | – G1 | – H4 | – I7 | – AB | – N1 | – D4 | – C7 | – LB | – M1 | – F4 | – P7 | – SB | – W1 | – Y4 | – V7 |
| GU | GUGA | GUUA | GUAA | GUCA | GUCU | GUAU | GUUU | GUGU | GUGC | GUUC | GUAC | GUCC | GUCG | GUAG | GUUG | GUGG |
| | – EC | – G2 | – H5 | – I8 | – AC | – N2 | – D5 | – C8 | – LC | – M2 | – F5 | – P8 | – SC | – W2 | – Y5 | – V8 |
| GA | GAGA | GAUA | GAAA | GACA | GACU | GAAU | GAUU | GAGU | GAGC | GAUC | GAAC | GACC | GACG | GAAG | GAUG | GAGG |
| | – ED | – G3 | – H6 | – I9 | – AD | – N3 | – D6 | – C9 | – LD | – M3 | – F6 | – P9 | – SD | – W3 | – Y6 | – V9 |
| UA | UAGA | UAUA | UAAA | UACA | UACU | UAAU | UAUU | UAGU | UAGC | UAUC | UAAC | UACC | UACG | UAAG | UAUG | UAGG |
| | – Q1 | – G4 | – H7 | – IA | – R1 | – N4 | – D7 | – CA | – K1 | – M4 | – F7 | – PA | – U1 | – W4 | - Y7 | – VA |
| AA | AAGA | AAUA | AAAA | AACA | AACU | AAAU | AAUU | AAGU | AAGC | AAUC | AAAC | AACC | AACG | AAAG | AAUG | AAGG |
| | – Q2 | – G5 | – H8 | – IB | – R2 | – N5 | – D8 | – CB | – K2 | – M5 | – F8 | – PB | – U2 | – W5 | – Y8 | – VB |
| CA | CAGA | CAUA | CAAA | CACA | CACU | CAAU- | CAUU | CAGU | CAGC | CAUC | CAAC | CACC | CACG | CAAG | CAUG | CAGG |
| | – Q3 | – G6 | – H9 | – IC | – R3 | N6 | – D9 | – CC | – K3 | – M6 | – F9 | – PC | – U3 | – W6 | – Y9 | – VC |

# Decryption Process

1. Generation of encoding table 1 & 2
2. Cipher text of protein sequence divided into 2 halves
3. Protein sequences converted to tRNA using amino acid table
4. tRNA converted to mRNA (Reverse Translation) Complement
5. mRNA converted to DNA (Reverse Transcription) U -> T
6. Multiple round functions are performed:
    a. DNA sequence XNOR with introns
    b. Left Shift the sequences
    c. DNA converted to mRNA (Transcription) T -> U
    d. mRNA to tRNA (translation process) complement
    e. tRNA to DNA (reverse transcription) U -> T
4. DNA transformed with introns
5. Transformed DNA converted to plaintext and merged

# References


- UbaidurRahman, N. H., Balamurugan, C., & Mariappan, R. (2015). A novel DNA computing based encryption and decryption algorithm. Procedia Computer Science, 46, 463-475.