INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 1)
Available online at www.ijariit.com

Data Encryption without Using Prime Numbers

Abhishek Kumar
abhishekkumar.jhansi@gmail.com

ABSTRACT

It is an encryption algorithm that uses randomly generated number sequences to encrypt data, instead of using prime numbers hence saving so much processing time, generating prime in itself a tedious task and required a heavy amount of computation , but generating random number sequences is far easier and require a significantly lesser amount of computation. This algorithm generates two random number sequences (discussed in introduction) (treated as private keys), digits in these number sequences are grouped in different configuration viz. 2 DG (grouping 2 digits), 3 DG (grouping 3 digits) this form groups of digits in both number sequences, these groups are then multiplied to form a result and this result is multiplied with plain data to encrypt the data.

1. ABBRIVIATIONS

DRNSBMRM2
D=decimal
R=random
N=number
S=sequence
B=bits
M=multiplier
R=resultant
M=multiplier
2=2 digit numbers up to 99

2. CRYPTOSYSTEM

1. Generate two RNS (random number sequence) from 01 to 99.
2. Say these random number sequences as RNS1 and RNS2.
3. RNS1 and RNS2 both have 198 bits decimal number sequence.
4. Group three bits together in both RNS1 and RNS2 until whole number sequence is grouped.
5. 66 groups are formed in both RNS1 and RNS2 (198/3).
6. Multiply group1 of RNS1 with group1 of RNS2 and obtain the result.
7. Multiply group2 of RNS1 and group2 of RNS2 and obtain the result.
8. Carry on this operation until all the groups in both RNS1 and RNS2 are multiplied.
9. Multiply the results which were obtained by above operations, we get a new result.
10. Multiply this result with data we get the encrypted data.

3. METHOD TO GENERATE RANDOM NUMBER SEQUENCES

3.1 Generate two digit random numbers from 01 to 99 for 99 times.(Each number is unique i.e. no duplicate numbers allowed)

3.2 Group them together to form a random number sequence.

4. EXAMPLE

Let the RNS1=999897……..69686766656463……01. (Max. value)
RNS2=999897……..69686766656463……01. (Max. value)
Grouping bits in both sequences
RNS1=999 897 969 594 ……..001.
Do similar with RNS2
RNS2=999 897 969 594 …….001.

Multiply groups of the sequences one by one as shown:-
999*999=998001(result1)
897*897=804609(result 2)
Carry on up to
001*001=01 (result 3)
Multiply all these results (result 1 and result 2 and so on) we get
59363275184755460138215867180695833778927761629789238030623651629653975563559733132009383771596429890773820174655156791770990970686782226815025245749390936234444115381139328011457243249866008078080164815775748785985985072047512479449977309896229465314695769382440533886883275872209097714204323272208091709440000000000000000000000000000000000000 (maximum possible value) (342 decimal bits)(Itself can be treated as a private key)

15120890936272247878926088402085514469934029238669722504633691744951297238468757385261079048102441132665130095798329460382860066477712272452115266616282923622677373891678161648295528491690335851693888659513724387237405100371201845551433708138920911250497802267417503988259303106958449049560027496339031310991360000000000000000000000000000000000 (minimum possible value) (340 decimal bits).
59212066275392737659426606296674978634228421337402540805577314712204462593971285739348327586678618577750730716507532384573270496403901099956981371908776264387217637799197151184662769040069697449291077594982437634726224456201039229489483393908233737418964598915569878348805734556151325280924832052257418857834086400000000000000000000000000000000 (342 decimal bits) (no. of keys possible).
Multiply this with data e.g. =256(maximum ASCII value).
(256*59363275184755460138215867180695833778927761629789238030623651629653975566355973313200938377159642989077382017465515679177099097068678222681502524574939093623444411538113932801145724324986600808078080164815775748785985985072047512479449977309896229465314695769382440533886883275872209097714204323272208091709440000000000000000000000000000000000 (maximum possible value)(342 decimal bits).
15196998447297397795383261998258133447405506977226044935839654817191417744987129168179440224552868605203809796471172013869337368849581625006464646291184407967601769353757166797093305427196569806798852219283859168921241217844416319473919419133343474312056211696190477667504211862328552901483630675768527147761664000000000000000000000000000000000 (342 decimal bits) are the encrypted data.

DECRYPTION
(15196998447297397795383261998258133447405506977226044935839654817191417744987129168179440224552868605203809796471172013869337368849581625006464646291184407967601769353757166797093305427196569806798852219283859168921241217844416319473919419133343474312056211696190477667504211862328552901483630675768527147761664000000000000000000000000000000000)/(59363275184755460138215867180695833778927761629789238030623651629653975566355973313200938377159642989077382017465515679177099097068678222681502524574939093623444411538113932801145724324986600808078080164815775748785985985072047512479449977309896229465314695769382440533886883275872209097714204323272208091709440000000000000000000000000000000000)=256.

5. CONCLUSION

The algorithm uses lesser computing power and is faster because it does not uses prime numbers for encryption method hence it is not secure enough if it is compared with algorithms those uses prime numbers.

6. REFERENCES

Computer Networks By -Behrouz A. Fourozan.

