Application of Factorial and Binomial identities in Cybersecurity

Chinnaraji Annamalai
School of Management, Indian Institute of Technology, Kharagpur, India
Email: anna@iitkgp.ac.in
https://orcid.org/0000-0002-0992-2584

Abstract: This paper focuses on the application of factorial and binomial identities in cybersecurity in connection with the symmetric and asymmetric encryptions. We can use the binomial identities and theorem in factorials as an effective security algorithm to protect the computing systems, programs, and networks.

MSC Classification codes: 05A10, 40A05 (65B10)

Keywords: binomial identity, cybersecurity, factorial, computing, networks

1. Introduction

Cybersecurity is the practice of protecting the computing systems, devices, networks, programs and data from cyber-attacks. Its objective is to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems and networks. For this purposes, we need a strong security mathematical algorithm like RSA algorithm and Elliptic Curve Cryptography. The factorial [1, 2] and binomial theorem [3, 4] will help to build a strong cryptographic algorithm for the effective information security.

2. Theorem in Factorials

The factorial of a non-negative integer *n*, denoted by *n*!, is the product of all positive integers less than or equal to *n*. For example, $5! = 1 \times 2 \times 3 \times 4 \times 5 = 120$ and $0! = 1$.

Theorem in Factorials [4] : $(n_1 + n_2 + n_3 + \cdots + n_k)! = T \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!$, where $T, n_i \in N = \{1, 2, 3, \cdots\}$ & $i = 1, 2, 3, \cdots, k$.

Proof: Let $x = n_2 + n_3 + \cdots + n_k$.
$(n_1 + x)! = n_1! \times (n_1 + 1)(n_1 + 2)(n_1 + 3) \cdots (n_1 + x)$.

We know that $(r + 1)(r + 2)(r + 3) \cdots (r + n) = a \times n!$, where a is a positive integer.

For example,

Let $n = 5$ and $r = 3$.

Then, $(3 + 1)(3 + 2)(3 + 3)(3 + 4)(3 + 5) = 6720 = 56 \times 120 = 56 \times 5!$

and $(5 + 1)(5 + 2)(5 + 3) = 336 = 56 \times 6 = 56 \times 3!$.

From the above result, we get $n_1! \times (n_1 + 1)(n_1 + 2) \cdots (n_1 + x) = a_1 \times n_1! \times x!$,

$i.e., (n_1 + x)! = a_1 \times n_1! \times x! = a_1 \times n_1! \times (n_2 + n_3 + \cdots + n_k)! \ (\because x = n_2 + n_3 + \cdots + n_k)$

Similarly, if we continue the same process up to *k*-1 times, then we obtain the below result.

$$(n_1 + n_2 + n_3 + \cdots + n_k)! = (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}) \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!.$$

Let $T = (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1})$, where $T, a_i \in N = \{1, 2, 3, \cdots\}$ & $i = 1, 2, 3, \cdots, k-1$.

Then $(n_1 + n_2 + n_3 + \cdots + n_k)! = T \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!$.

3. Cybersecurity

The following result can be used in a strong security algorithm on the symmetric and asymmetric encryptions in the field of cryptography and cybersecurity in order to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems and networks.

$$(n_1 + n_2 + n_3 + \cdots + n_k)! = (a_1 \times a_2 \times a_3 \times \cdots \times a_{k-1}) \times n_1! \times n_2! \times n_3! \times \cdots \times n_k!.$$

Also, the binomial identities mentioned below can be used in cybersecurity:

(1) $V_r^n = V_n^r$ $(n, r \geq 1$ & $n, r \in N)$. (2) $V_r^{n+1} - V_r^n = V_{r-1}^n$.

(3) $1 + V_1^1 + V_1^2 + V_1^3 \cdots \cdots V_1^n = V_2^n$. (4) $V_n^n = 2V_{n-1}^n$.

(5) $V_0^n + V_1^n + V_2^n + V_3^n \cdots + V_{r-1}^n + V_r^n = V_r^{n+1}$.

The numerical expression of binomial coefficient [3] used in binomial identities is given below:

$$V_r^n = \frac{(r+1)(r+2)(r+3)\cdots\cdots(r+n-1)(r+n)}{n!}, (n, r \in N, n \geq 1, \& \, r \geq 0).$$

4. Conclusion

In this article, a mathematical model for an effective security algorithm has been introduced in order to protect the computing systems, devices, networks, programs and data from cyber-attacks. Its objective is to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, programs, and networks.

References

[1] McCulloch J F (1888) "A Theorem in Factorials", Annals of Mathematics, Vol. 4(5), pp 161-163. https://doi.org/10.2307/1967449.

[2] Bhargava M (2008) "The Factorial Function and Generalizations", The American Mathematical Montly", Vol. 107 (9), pp 783 – 199. https://doi.org/10.1080/00029890.2000.12005273

[3] Annamalai C (2022) "Annamalai's Binomial Identity and Theorem", SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.4097907.

[4] Annamalai C (2022) "Theorems based on Annamalai's Binomial Coefficient and Identity", Zenodo. https://doi.org/10.5281/zenodo.6548228.