

A. विशेषज्ञ का विवरण (Expert Details)

- नाम: नीता मिश्रा
- पदनाम: टीजीटी (TGT)
- विद्यालय का नाम: सुरेंद्रनाथ सेंटेंनरी स्कूल, रांची
- राज्य / देश: झारखंड / भारत
- विशेषज्ञता का क्षेत्र: गणित (Mathematics)

B. संसाधन का विवरण (Resource Details)

- ट्यूटोरियल शीर्षक: घातों की घात (The powers of powers)
- प्रौद्योगिकी / उपकरण: स्प्रेडशीट (Spreadsheet), पासा (Dice), कास्पर्स्की पासवर्ड टेस्टर (Kaspersky Password Testers), कैनवा (Canva), एक्समाइंड (Xmind), गूगल स्लाइड (Google Slide), गूगल शीट (Google Sheet)
- लक्षित शिक्षार्थी: कक्षा 8
- अनुमानित अवधि: 3 घंटे

सीखने के उद्देश्य (Learning Objectives)

1. गणना के मूलभूत सिद्धांत (Fundamental Counting Principle) और घातांक (Exponent) के वास्तविक जीवन में अनुप्रयोग को प्रदर्शित करना।
2. भौतिक सुरक्षा (Physical Security) और डिजिटल सुरक्षा (Digital Security) के बीच अंतर स्पष्ट करना।
3. आधार (Base) और लंबाई की घात (Power of length) के चरों का विश्लेषण करना।
4. विद्यार्थियों को गणितीय साक्ष्यों के साथ सशक्त बनाना।

अपेक्षित शिक्षण परिणाम (Expected Learning Outcomes)

1. गणना के मूलभूत सिद्धांत का उपयोग करके वास्तविक जीवन की परिस्थितियों के लिए कुल संभावित संयोजनों (Combinations) की गणना करना।
2. घातों का उपयोग करके संयोजन उपकरण तैयार करना।
3. संयोजनों को प्रदर्शित करने के लिए ट्री आरेख (Tree Diagrams) बनाना।
4. किसी कंप्यूटर द्वारा पासवर्ड क्रैक करने में लगने वाले सटीक समय की गणना करना।
5. विभिन्न सुरक्षा विधियों की गणितीय मजबूती की तुलना करना।
6. अपने परिवार और समुदाय की डिजिटल सुरक्षा का ऑडिट करना।

C. समस्या कथन (Problem Statement)

प्रतिदिन लोग अपने खातों के हैक होने की समस्या का सामना करते हैं क्योंकि वे कमजोर पासवर्ड का उपयोग करते हैं। मुख्य समस्या यह है कि हम कंप्यूटर पासवर्ड को भी भौतिक तालों की तरह ही समझते हैं। 3-अंकों वाला ताला साइकिल या सूटकेस के लिए बिल्कुल सही काम करता है क्योंकि इंसानी हाथ धीमे होते हैं और हर संयोजन को आजमाने में काफी समय लगता है। लेकिन हैकर्स स्वचालित कंप्यूटर प्रोग्रामों का उपयोग करते हैं जो एक सेकंड में लाखों पासवर्ड का अनुमान लगा सकते हैं।

चूंकि हममें से अधिकांश लोग इसके पीछे के गणित को नहीं समझते कि कंप्यूटर कितनी तेजी से अनुमान लगा सकते हैं, इसलिए हम ऐसे पासवर्ड बनाते हैं जो बहुत छोटे और बहुत सरल होते हैं। यह केस पेपर आधार (Base) और घात (Power) का विश्लेषण करने के लिए कक्षा 8 के गणित—संयोजन और घात—का उपयोग करेगा।

D. प्रस्तावित समाधान (Proposed Solution)

- **अंकों और प्रतीकों की तुलना में लंबाई को प्राथमिकता:** गणित यह साबित करता है कि पासवर्ड को भ्रमित करने वाला या जटिल बनाने की तुलना में उसे लंबा बनाना कहीं अधिक बेहतर है। घातांक के काम करने के तरीके के कारण, केवल कुछ और वर्ण (Characters) जोड़ने से ही संभावित संयोजनों की संख्या में भारी उछाल आता है। हमें यह समझने की जरूरत है कि एक लंबा और सरल पासवर्ड एक ऐसी गणितीय पहेली खड़ी करता है जिसे हैकर के कंप्यूटर के लिए हल कर पाना असंभव के करीब होता है।
- **"4-शब्दों वाला पासफ्रेज़" (4-word passphrase) तरीका:** एक छोटे पासवर्ड का उपयोग करने के बजाय, सबसे अच्छा समाधान 4 यादृच्छिक, सामान्य दैनिक शब्दों से बना एक पासफ्रेज़ उपयोग करना है (उदाहरण के लिए: river-apple-shoe-planet)। इंसानों के लिए इसकी कल्पना करना और याद रखना बहुत आसान है, लेकिन एक कंप्यूटर के लिए, 20 अक्षरों का यह वाक्यांश खरबों-खरब संयोजन बना देता है, जिसका अनुमान लगाने में युगों का समय लग जाएगा।

E. आवश्यक उपकरण (Tools Required)

- Xmind
- Google Sheet
- Gemini Notebook

F. चरण-दर-चरण प्रदर्शन (Step-by-Step Demonstration)

उदाहरण 1: वार्डरोब की स्थिति (गणना का मूलभूत सिद्धांत)

जॉन अपने दैनिक कपड़ों को व्यवस्थित कर रहा है। वह यादृच्छिक रूप से कपड़े चुनने के बजाय हर संभव अनूठे संयोजन का निर्धारण करना चाहता है जिसे वह पहन सकता है।

आइए चरों (Variables) की पहचान करें:

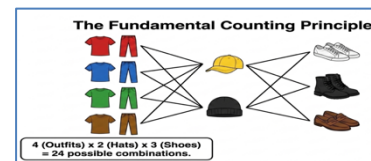
- **चर 1: बेस लेयर (पोशाक/ड्रेस सेट):** उसके पास 4 अलग-अलग मोनोक्रोम सेट हैं - लाल, नीला, हरा और भूरा ($n_1 = 4$)।
- **चर 2: हेडवियर (टोपी):** उसके पास 2 टोपियां हैं - एक पीली बेसबॉल कैप और एक काली बीनी ($n_2 = 2$)।
- **चर 3: फुटवियर (जूते):** उसके पास 3 जोड़ी जूते हैं - सफेद स्नीकर्स, काले जूते और भूरे लोफर्स ($n_3 = 3$)।

गणितीय प्रदर्शन:

- **चरण 1: (पोशाक और टोपियां):** ट्री आरेख के अनुसार, 2 टोपियां और 4 पोशाकें = $2 \times 4 = 8$ अनूठे संयोजन (प्रत्येक 1 टोपी के लिए, 4 अनूठी पोशाकें हैं।)
- **चरण 2: (जूते जोड़ना):** यदि हम फुटवियर के 3 सेट जोड़ते हैं:
 $4 \text{ (पोशाकें)} \times 2 \text{ (टोपियां)} \times 3 \text{ (जूते)} = 24$ संभावित संयोजन।

गणना का मूलभूत सिद्धांत (Fundamental Counting Principle):

यदि घटना 1, m तरीकों से घटित हो सकती है, घटना 2, n तरीकों से घटित हो सकती है, और घटना 3, p तरीकों से घटित हो सकती है, तो कुल संयोजन = $m \times n \times p$



स्वयं हल करें (Figure it Out):

रिया के पास 7 ड्रेस, 5 टोपियां और 6 जोड़ी जूते हैं। रिया कितने अलग-अलग तरीकों से तैयार हो सकती है?

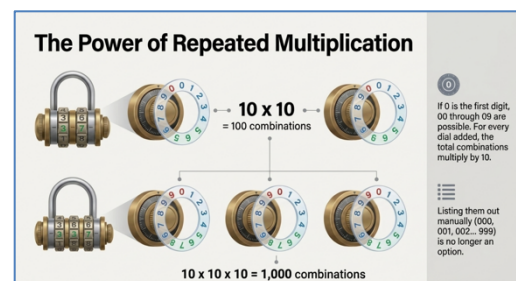
(उत्तर: $7 \times 5 \times 6 = 210$ तरीके)

उदाहरण 2: भौतिक तालों की जांच (घातांक / Exponents)

2A: 2-अंकों वाला ताला (खिलौना तिजोरी)

चर:

- पहिया 1 (दहाई का स्थान): 10 संभावित अंक (0 से 9)
- पहिया 2 (इकाई का स्थान): 10 संभावित अंक (0 से 9)



गणितीय प्रदर्शन:

गणना के मूलभूत सिद्धांत के अनुसार:

कुल संयोजन = $10 \times 10 = 100$

एक 2-अंकों के कोड को 2-आयामी (2D) ग्रिड पर देखा जा सकता है। पहिया 1 के 10 मानों को पंक्तियों (rows) में और पहिया 2 के 10 मानों को स्तंभों (columns) में रखने पर $10 \times 10 = 100$ प्रतिच्छेदक सेल बनते हैं।

- मानव क्रैकिंग समय बनाम कंप्यूटर क्रैकिंग समय:

यदि कोई अनधिकृत व्यक्ति प्रति 1.5 सेकंड में 1 कोड मैनुअल रूप से डायल करता है:

कुल समय = 100×1.5 सेकंड = 150 सेकंड = 2.5 मिनट।

जबकि एक कंप्यूटर प्रति सेकंड 10,000 कोड जांचता है: समय = $100 / 10000 = 0.01$ सेकंड।

- निष्कर्ष: 2-अंकों का ताला लगभग शून्य सुरक्षा प्रदान करता है क्योंकि कोई भी इसे बिना किसी उपकरण के 3 मिनट से भी कम समय में क्रैक कर सकता है।

2B: 3-अंकों वाला ताला (सूटकेस/लगेज लॉक)

- पहिया 1 (सैकड़े का स्थान): 10 संभावित अंक (0 से 9)
- पहिया 2 (दहाई का स्थान): 10 संभावित अंक (0 से 9)
- पहिया 3 (इकाई का स्थान): 10 संभावित अंक (0 से 9)

गणितीय प्रदर्शन:

जब तीसरा पहिया जोड़ा जाता है, तो पिछले 100 संयोजनों में से प्रत्येक 10 नई संभावनाओं से जुड़ जाता है:

कुल संयोजन = $10 \times 10 \times 10 = 10^2 \times 10 = 10^3 = 1,000$ (000 से 999 तक)

तालिका 1: भौतिक तालों की तुलना

लॉक का प्रकार	आधार (Base)	लंबाई (Length)
2-अंकों का लॉक	10	2
3-अंकों का लॉक	10	3
4-अंकों का लॉक	10	4

स्वयं हल करें (5-अंकों वाला सुरक्षित ताला):

- कुल संयोजन कितने होंगे? ($10^5 = 100,000$)
- मानव समय (मिनटों में): ($100,000 \times 1.5 / 60 = 2,500$ मिनट)
- कंप्यूटर समय (सेकंडों में): ($100,000 / 10,000 = 10$ सेकंड)

उदाहरण 3: डिजिटल छलांग – पासवर्ड संयोजन और क्रैकिंग गति

- 3.1 4-अंकों का पिन (केवल संख्याएँ):
आधार $b = 10$ (0 से 9), लंबाई $L = 4$

$$\text{कुल संयोजन} = 10 \times 10 \times 10 \times 10 = 10^4 = 10,000$$

$$\text{क्रेक करने का समय (10,000 अनुमान/सेकंड पर)} = 10,000 / 10,000 = 1 \text{ सेकंड}$$

- **3.2 एक अंक को छोटे अक्षर (a-z) से बदलना:**

पहले स्थान पर 26 (a-z) विकल्प, शेष 3 स्थानों पर 10 संख्यात्मक (0-9) विकल्प

$$\text{कुल संयोजन} = 26 \times 10 \times 10 \times 10 = 26,000 \text{ संयोजन}$$

$$\text{क्रेक करने का समय} = 26,000 / 10,000 = 2.6 \text{ सेकंड (2.6 गुना वृद्धि)}।$$

- **3.3 प्रत्येक स्थान पर संख्या (0-9) या छोटा अक्षर (a-z) होना:**

$$\text{आधार } b = 10 + 26 = 36, \text{ लंबाई } L = 4$$

$$\text{कुल संयोजन} = 36 \times 36 \times 36 \times 36 = 36^4 = 1,679,616$$

$$\text{क्रेक करने का समय} = 1,679,616 / 10,000 \approx 168 \text{ सेकंड (168 गुना वृद्धि)}।$$

- **स्वयं हल करें:**

यदि प्रत्येक स्थान पर अंक (0-9), छोटा अक्षर (a-z) या बड़ा अक्षर (A-Z) हो, तो कुल संयोजन कितने होंगे?

$$(\text{आधार } b = 10 + 26 + 26 = 62; \text{ कुल संयोजन} = 62^4 = 14,776,336)$$

गणितीय बदलाव की व्याख्या:

इस तालिका के अध्ययन से स्पष्ट होता है कि वर्णों की विविधता जोड़ने से आधार (b) बढ़ता है, लेकिन वर्णों की लंबाई बढ़ाने से घातांक (L) बढ़ता है। सामान्य शब्दों से बना 16-वर्णों का पासवर्ड (जैसे: river-apple-Bombay-nest) जटिल प्रतीकों से भरे 8-वर्णों के पासवर्ड की तुलना में 70 लाख गुना बड़ी गणितीय चुनौती प्रस्तुत करता है।

G. अपेक्षित परिणाम (Expected Output)

1. गणना के मूलभूत सिद्धांत का उपयोग करके वास्तविक दुनिया की परिस्थितियों के लिए कुल संभावित संयोजनों की गणना करना।
2. घातों का उपयोग करके संयोजन उपकरण तैयार करना।
3. संयोजनों को प्रदर्शित करने के लिए ट्री आरेख बनाना।
4. कंप्यूटर द्वारा पासवर्ड क्रेक करने में लगने वाले सटीक समय की गणना करना।

H. अभिनव विस्तार (Innovation Extension)

1. एक पास को 6 बार फेंककर 6 अंकों का कोड बनाएं और शीर्ष पर आने वाले अंक को लिखें (जैसे: 351623, 112356)।
2. वास्तविक व्यक्तिगत पासवर्ड को रिकॉर्ड किए बिना, परिवार के उपकरणों में पासवर्ड की लंबाई (L) और वर्ण पूल के आधार (b) पर एक छात्र-नेतृत्व वाला सर्वेक्षण आयोजित करें और निष्कर्षों को बारंबारता वितरण तालिकाओं (Frequency Distribution Tables) और बार ग्राफ (Bar Graphs) में व्यवस्थित करें। इसे क्रिटिकल (गंभीर), मॉडरेट (मध्यम) और सिव्योर (सुरक्षित) श्रेणियों में वर्गीकृत करें।

I. संदर्भ (References)

1. गणित प्रकाश (कक्षा 8)
2. कम्प्यूटेशनल थिंकिंग एवं एआई हैंडबुक (CBSE)
3. साइबर सुरक्षा रूपरेखा (Cybersecurity Frameworks)
4. जेमिनी नोटबुक (Gemini Notebook)