নাম: _____ তারিখ: _____ নম্বর: _____

# কীভাবে আপনার IP ঠিকানা লুকাবেন ওয়ার্কশিট

IP ঠিকানা লুকানো, অবস্থান মাস্কিং, প্রক্সি, Tor এবং DNS/WebRTC ফাঁস প্রতিরোধ

## VPN শিক্ষণ সারসংক্ষেপ

**শিক্ষার্থী**
**শিক্ষার্থী স্ট্যাটাস**
নেটওয়ার্ক ডিফেন্ডার ট্র্যাক

**নিরাপদ**
**সংযোগের অবস্থা**
ডেটা প্যাকেট সুরক্ষিত রাখা

**সক্রিয়**
**লিক সুরক্ষা**
DNS ও IPv6 লিক সুরক্ষা

**স্বাগতম!** এই অ্যাক্টিভিটি প্যাকেট আপনাকে ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN)-এর মৌলিক নীতি বিষয়ে গাইড করবে। আপনি জানবেন এনক্রিপ্টেড টানেল কীভাবে আপনার ডেটা সুরক্ষিত করে, নেটওয়ার্ক প্রোটোকল কীভাবে কাজ করে এবং গোপনীয়তা লিক কীভাবে শনাক্ত ও প্রশমিত করবেন।

**ওয়ার্কশিট চেকপয়েন্ট**

- [ ] **অংশ 1-4: VPN-এর ধারণা ও প্রোটোকলে দক্ষতা অর্জন করুন।**
- [ ] **অংশ 5-7: ক্রসওয়ার্ড ও ওয়ার্ড সার্চ ধাঁধা সমাধান করুন।**
- [ ] **অংশ 8-9: কেস স্টাডি ও সংকেতবার্তা চ্যালেঞ্জ সমাধান করুন।**
- [ ] **অংশ 10: প্রাথমিক ও উন্নত স্তরের FAQ পেজ পর্যালোচনা করুন।**
- [ ] **অংশ 11: 10টি আকর্ষণীয় বাস্তব তথ্য অন্বেষণ করুন।**
- [ ] **অতিরিক্ত: দ্রুত ভাবুন চ্যালেঞ্জ।**

**VPN.com VPN গাইড খুলুন**

URL: https://www.vpn.com/bn/vpn/

# আপনার VPN শেখার রোডম্যাপ

- IP ঠিকানা কীভাবে কাজ করে এবং কীভাবে অবস্থান ফাঁস করে তা ব্যাখ্যা করুন।
- নেটওয়ার্ক ঠিকানা আড়াল করার ক্ষেত্রে প্রক্সি, Tor ও VPN-এর পার্থক্য তুলনা করুন।
- DNS ও WebRTC ফাঁস শনাক্ত ও প্রতিরোধের পদ্ধতিগুলো শনাক্ত করুন।
- ওয়েবসাইট কীভাবে পাবলিক IP-র মাধ্যমে ব্যবহারকারীদের ট্র্যাক করে তা বুঝুন।
- IP সুরক্ষার জন্য মাল্টি-হপ রাউটিং ও এনক্রিপ্টেড টানেল মূল্যায়ন করুন।

## IP সুরক্ষা ওয়ার্কশিটের নির্দেশনা

বহুনির্বাচনী ও সত্য/মিথ্যা প্রশ্নের উত্তর দিন, শব্দভাণ্ডার ব্যবহার করে শূন্যস্থান পূরণ করুন, সংজ্ঞা মেলান এবং ক্রসওয়ার্ড ও শব্দ খোঁজার ধাঁধা সমাধান করুন। আপনার IP ঠিকানা লুকানো ও লিক প্রতিরোধ বিষয়ে আপনার জ্ঞান প্রয়োগ করুন। শেষে অতিরিক্ত কার্যক্রম দ্রুত ভাবুন সম্পন্ন করুন।

## আপনার IP লুকানো (ভূমিকা)

আপনার IP ঠিকানা একটি ডিজিটাল ডাক-ঠিকানা, যা আপনার ভৌত অবস্থান ও নেটওয়ার্ক-অভ্যাস প্রকাশ করে। আপনার IP লুকানো অনলাইন ট্র্যাকিং, লক্ষ্যভিত্তিক প্রোফাইলিং ও ভৌগোলিক ব্লকিংয়ের বিরুদ্ধে প্রথম প্রতিরক্ষা। নিরাপদে আপনার ঠিকানা আড়াল করার উপায় বোঝা অনলাইনে আপনার গোপনীয়তা রক্ষায় সাহায্য করে।

**প্রতিটি চেকপয়েন্ট মনোযোগ দিয়ে পড়ুন এবং সঠিক উত্তরটি বেছে নিন বা লিখুন।**

# চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1. আপনার ভিজিট করা ওয়েবসাইটগুলোর কাছে একটি ডিভাইসের পাবলিক IP অ্যাড্রেস কী প্রকাশ করে?

- A. ব্যবহারকারীর ক্রেডিট কার্ড নম্বর
- B. আপনার আনুমানিক অবস্থান এবং ISP-র নাম
- C. সম্পূর্ণ লোকাল ফাইল ডিরেক্টরি
- D. কীবোর্ডের ভাষা সেটিংস

2. কোন পদ্ধতি আপনার IP লুকায় এবং সিস্টেমজুড়ে সব ট্রাফিক এনক্রিপ্ট করে?

- A. একটি সাধারণ ওয়েব প্রক্সি
- B. আপনার ব্রাউজারের কুকি মুছে ফেলা
- C. একটি ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN)
- D. আপনার নেটিভ ফায়ারওয়াল নিষ্ক্রিয় করা

3. ফ্রি ওয়েব প্রক্সি ব্যবহারের একটি প্রধান গোপনীয়তাগত সীমাবদ্ধতা কী?

- A. এটি পাবলিক নেটওয়ার্কে ডেটা ট্রাফিক এনক্রিপ্ট করে না
- B. এর জন্য একটি বাহ্যিক অপারেটিং সিস্টেম ইনস্টল করতে হয়
- C. যুক্তরাষ্ট্রে এটি সম্পূর্ণ বেআইনি
- D. এর জন্য একটি ডেডিকেটেড টেলিফোন লাইন সংযোগ লাগে

4. Tor নেটওয়ার্ক ব্যবহারকারীদের উচ্চ বেনামিত্ব কীভাবে দেয়?

- A. সংযোগের গতি বাড়িয়ে
- B. স্বেচ্ছাসেবীদের চালানো তিনটি রিলের মধ্য দিয়ে ট্রাফিক পাঠিয়ে
- C. বৈশ্বিক ডেটাবেসে আপনার নাম নিবন্ধন করে
- D. শুধু সরকারি সংস্থাগুলোর জন্য অ্যাক্সেস সীমিত করে

5. DNS লিক কী?

- A. ভুল ঠিকানায় ইমেইল পাঠানোর ত্রুটি
- B. যখন DNS কোয়েরি VPN টানেল এড়িয়ে ISP-র কাছে যায়
- C. স্থানীয় রাউটারের পাওয়ার সাপ্লাইয়ের হার্ডওয়্যার ব্যর্থতা
- D. স্থানীয় নেটওয়ার্ক অ্যাডাপ্টার ড্রাইভারের একটি হালনাগাদ

# চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

### 6 প্রশ্ন 6

6. প্রক্সি সার্ভার VPN-এর মতোই ব্যাকগ্রাউন্ড OS ট্রাফিক এনক্রিপ্ট করে।

○ সত্য ○ মিথ্যা

### 7 প্রশ্ন 7

7. Tor রাউটিং অত্যন্ত নিরাপদ, কিন্তু নেটওয়ার্ক ব্রাউজিংয়ের গতি কমায়।

○ সত্য ○ মিথ্যা

### 8 প্রশ্ন 8

8. সক্রিয় VPN সেশনের সময় WebRTC লিক আপনার আসল IP প্রকাশ করে দিতে পারে।

○ সত্য ○ মিথ্যা

### 9 প্রশ্ন 9

9. VPN চালু থাকলে এবং কোনো ফাঁস না থাকলে আপনার ISP দেখতে পায় না আপনি কোন ওয়েবসাইটে যান।

○ সত্য ○ মিথ্যা

### 10 প্রশ্ন 10

10. আপনার IP ঠিকানা লুকালে ব্রাউজার ফিঙ্গারপ্রিন্টিংয়ের মাধ্যমে ট্র্যাকিং ব্লক হয়।

○ সত্য ○ মিথ্যা

## চেকপয়েন্ট 3: মূল পরিভাষা বসানো

নিচের প্রতিটি বাক্য পড়ুন এবং ওয়ার্ড ব্যাংক থেকে সঠিক শব্দ দিয়ে শূন্যস্থান পূরণ করুন।

1. নিরাপদ টানেল এড়িয়ে আপনার ডোমেইন কোয়েরি প্রকাশ করে দেওয়াকে বলা হয় _____।

2. ব্রাউজারভিত্তিক _____ যোগাযোগ API অসাবধানে আপনার আসল আইপি ঠিকানা ফাঁস করে দিতে পারে।

3. ওয়েব _____ ব্রাউজার ট্র্যাফিক পুনঃনির্দেশ করে, কিন্তু প্যাকেটের পেলোড এনক্রিপ্ট করে না।

4. _____ নেটওয়ার্কের বহুস্তরীয় এনক্রিপশন উচ্চমাত্রার বেনামিত্ব দেয়।

5. আপনার পাবলিক _____ টেলিকম প্রদানকারী নির্ধারণ করে এবং তা আপনার এলাকা প্রকাশ করে।

6. আঞ্চলিক মিডিয়া-নিষেধাজ্ঞা এড়ানো সম্ভব হয় _____ মাস্কিংয়ের মাধ্যমে।

### পরিভাষা শব্দভাণ্ডার

আইএসপি ট্র্যাকিং | আইপি ঠিকানা | টর | ডিএনএস লিক | প্রক্সি | ভিপিএন টানেল | লোকেশন | WebRTC

**এখানে আপনার উত্তর লিখুন:**

1. 
2. 
3. 
4. 
5. 
6. 

# চেকপয়েন্ট 4: নেটওয়ার্ক ধারণা মিলান

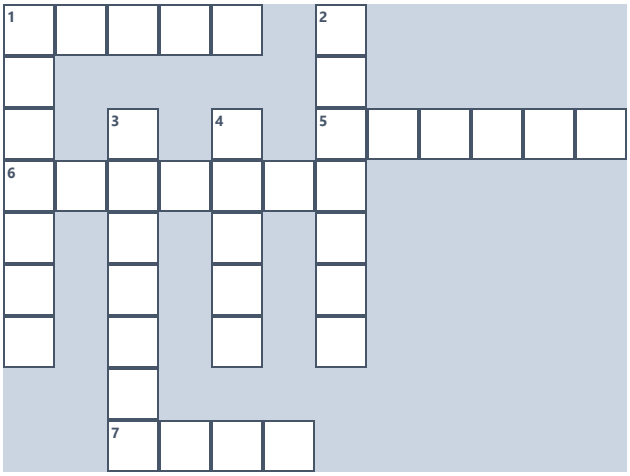
**সংজ্ঞা মেলানো**

পূরণযোগ্য ইনপুট বক্সে সংশ্লিষ্ট অক্ষর (A-H) লিখে বামদিকের প্রতিটি শব্দভাণ্ডার-পদকে ডানদিকের সঠিক সংজ্ঞার সঙ্গে মেলান।

| | | | |
|---|---|---|---|
| ☐ | **1. IP ঠিকানা** | **A** | ডিভাইসের সব ট্রাফিক এনক্রিপ্ট করে এবং একটি VPN সার্ভারের মধ্য দিয়ে পাঠায়। |
| ☐ | **2. VPN টানেল** | **B** | তিনটি স্বেচ্ছাসেবী সার্ভারের মধ্য দিয়ে ডেটা পাঠায় এবং প্রতিটি ধাপে স্তর এনক্রিপ্ট করে। |
| ☐ | **3. Tor নেটওয়ার্ক** | **C** | জিও-ব্লক এড়াতে অন্য দেশের সার্ভারের মধ্য দিয়ে সংযোগ পাঠানো। |
| ☐ | **4. ওয়েব প্রক্সি** | **D** | ইন্টারনেটে একটি ডিভাইস ইন্টারফেস শনাক্তকারী অনন্য সংখ্যাসূচক লেবেল। |
| ☐ | **5. DNS লিক** | **E** | সিস্টেম এনক্রিপশন ছাড়াই অ্যাপ্লিকেশন স্তরে ব্রাউজার ট্রাফিক পুনঃনির্দেশ করে। |
| ☐ | **6. WebRTC API** | **F** | আপনার টেলিকম কর্তৃক এনক্রিপ্ট-না-করা ইন্টারনেট ট্রাফিকের গন্তব্যের লগ রাখা। |
| ☐ | **7. অবস্থান আড়াল করা** | **G** | যে কোয়েরি VPN টানেলের বাইরে রেজলভ হয় এবং ISP-র কাছে দেখা ডোমেইন প্রকাশ করে দেয়। |
| ☐ | **8. ISP ট্র্যাকিং** | **H** | ভয়েস/ভিডিওর জন্য ব্রাউজারের বৈশিষ্ট্য, যা টানেল এড়িয়ে আপনার আসল IP ঠিকানা প্রকাশ করে দিতে পারে। |

## চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

সক্রিয় সাদা ঘরে অক্ষর লিখে ক্রসওয়ার্ড পাজল সমাধান করুন। সংখ্যাগুলো নিচের সূত্রের সঙ্গে মেলে।




### পাশাপাশি

**1. সিস্টেম-এনক্রিপশন ছাড়া অ্যাপ্লিকেশন স্তরে ব্রাউজার ট্র্যাফিক পুনঃনির্দেশ করে (5)**

**5. তথ্যকে অন্যের কাছে অপাঠ্য কোডে রূপান্তরের পদ্ধতি (6)**

**6. ইন্টারনেটে ডিভাইসের ইন্টারফেস শনাক্তকারী অনন্য সংখ্যাসূচক লেবেল (7)**

**7. নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4)**

### উপর-নিচ

**1. ভয়েস ও ভিডিওর ব্রাউজার ফিচার, যা টানেল এড়িয়ে আসল আইপি ঠিকানা ফাঁস করতে পারে (7)**

**2. আপনার টেলিকম প্রদানকারীর অনএনক্রিপ্টেড ইন্টারনেট ট্র্যাফিকের গন্তব্য লগ করা (7)**

**3. ডিভাইসের সব ট্র্যাফিক এনক্রিপ্ট করে ভিপিএন সার্ভার দিয়ে পাঠায় (7)**

**4. সেবা ব্যবহারের জন্য তৈরি ব্যক্তিগত নিবন্ধন (5)**

# চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

স্ক্রিন-রিডার ও কিবোর্ড ব্যবহারকারীরা নিচের টেক্সট ফিল্ডে সরাসরি ক্রসওয়ার্ডের উত্তর লিখতে পারেন।

## পাশাপাশি

**1 পাশাপাশি: সিস্টেম-এনক্রিপশন ছাড়া অ্যাপ্লিকেশন স্তরে ব্রাউজার ট্র্যাফিক পুনঃনির্দেশ করে (5 অক্ষর):**

**5 পাশাপাশি: তথ্যকে অন্যের কাছে অপাঠ্য কোডে রূপান্তরের পদ্ধতি (6 অক্ষর):**

**6 পাশাপাশি: ইন্টারনেটে ডিভাইসের ইন্টারফেস শনাক্তকারী অনন্য সংখ্যাসূচক লেবেল (7 অক্ষর):**

**7 পাশাপাশি: নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4 অক্ষর):**

## উপর-নিচ

**1 উপর-নিচ: ভয়েস ও ভিডিওর ব্রাউজার ফিচার, যা টানেল এড়িয়ে আসল আইপি ঠিকানা ফাঁস করতে পারে (7 অক্ষর):**

**2 উপর-নিচ: আপনার টেলিকম প্রদানকারীর অনএনক্রিপ্টেড ইন্টারনেট ট্র্যাফিকের গন্তব্য লগ করা (7 অক্ষর):**

**3 উপর-নিচ: ডিভাইসের সব ট্র্যাফিক এনক্রিপ্ট করে ভিপিএন সার্ভার দিয়ে পাঠায় (7 অক্ষর):**

**4 উপর-নিচ: সেবা ব্যবহারের জন্য তৈরি ব্যক্তিগত নিবন্ধন (5 অক্ষর):**

## চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

নিচের গ্রিডে লুকানো ৪টি মূল শব্দভাণ্ডারের শব্দ খুঁজুন। শব্দগুলো অনুভূমিক, উল্লম্ব বা কোণাকুণি হতে পারে।

ক সি দ ঠ হ সা শ মে দে রা কি ঋ তে না নে
ছ য ক্সি প উ অ উ ঋ আ মা বা য ফ বা ম
দে তি প্র ভ ঘ রে ষ ফ ঘ ই দ হ স ভ রি
মি ঢ ব ন শ প ক্রি ন এ ষ এ ষ রি সি না
তি তা য়ে ড ঊ আ নি রা কি থ সে স ঊ লি গ
সি নি ও জা পি ই ঋ ভি জি ন্ট লি ট পি ভ ণ
টি জে গ স ঘ পি রে দি পি মি উ ঋ পা ট্র্যা উ
র অ জে কা গ অ্ ম আ ঘ এ কি কা ঘ ঝ কিং
আ ণ ধ গ সি যা রি শ ছ দ ন সে যা জি নি
ব ঝ রে পে জ ড্রে ল আ আ রে মা টা স অ্ মে
য়ে তি দে রি ফ স গ সি তি সে খ স নে বে উ
ও ট সে দি দা প ই আ সি জে বি বি য ল ড
দ ষ সা ফ ল ল ন তা কে ণ রা রি ণ জে ই
কে পে ঠ পি ঊ বে সে বে উ ণ ল জে ঢ ফ কি
মে কা দা ঋ ল জে বে ঠ বি কে লে পা ম পি মি

### পরিভাষা শব্দতালিকা

আইপিঅ্যাড্রেস ভিপিএনটানেল ওয়েবপ্রক্সি ওয়েবআরটিসি আইএসপিট্র্যাকিং লগইন
এনক্রিপশন অ্যাকাউন্ট

# চেকপয়েন্ট 6, বিকল্প: সহজবোধ্য শব্দভাণ্ডার মিলান

ফাঁকা জায়গায় অক্ষর (A-H) লিখে ওয়ার্ড সার্চের ৪টি শব্দভাণ্ডার-পদের প্রতিটিকে তার সঠিক সংজ্ঞার সঙ্গে মেলান।

**পরিভাষা**

**A. আইপিঅ্যাড্রেস**

**B. ভিপিএনটানেল**

**C. ওয়েবপ্রক্সি**

**D. ওয়েবআরটিসি**

**E. আইএসপিট্র্যাকিং**

**F. লগইন**

**G. এনক্রিপশন**

**H. অ্যাকাউন্ট**

**সংজ্ঞা ও মিলের ঘর**

1. ভয়েস ও ভিডিওর ব্রাউজার ফিচার, যা টানেল এড়িয়ে আসল আইপি ঠিকানা ফাঁস করতে পারে।

2. তথ্যকে অন্যের কাছে অপাঠ্য কোডে রূপান্তরের পদ্ধতি।

3. নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া।

4. ইন্টারনেটে ডিভাইসের ইন্টারফেস শনাক্তকারী অনন্য সংখ্যাসূচক লেবেল।

5. সিস্টেম-এনক্রিপশন ছাড়া অ্যাপ্লিকেশন স্তরে ব্রাউজার ট্র্যাফিক পুনঃনির্দেশ করে।

6. সেবা ব্যবহারের জন্য তৈরি ব্যক্তিগত নিবন্ধন।

7. আপনার টেলিকম প্রদানকারীর অনএনক্রিপ্টেড ইন্টারনেট ট্র্যাফিকের গন্তব্য লগ করা।

8. ডিভাইসের সব ট্র্যাফিক এনক্রিপ্ট করে ভিপিএন সার্ভার দিয়ে পাঠায়।

## চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

VPN-এর মূল ধারণা ও পরিভাষা জানতে নিচের অক্ষরগুলো সাজান। উত্তর পূরণযোগ্য ইনপুট বাক্সে লিখুন।

1. অ্ড্রে আ যা স পি ই _____

2. ও ক্সি প্র ব য়ে _____

3. স আ পি কিং এ ট্র্যা ই _____

4. ন প ক্রি শ এ ন _____

5. টা ল ন এ ভি নে পি _____

6. টি ব র ও আ সি য়ে _____

7. ই ল ন গ _____

8. ন্ট অ্ কা উ যা _____

# অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

প্রতিটি বিভাগে ৩টি উত্তর। যে প্রথমে তালিকা পূরণ করবে, সে জিতবে।

| | | | | |
|---|---|---|---|---|
| 1 | ভ্রমণের সময় VPN ব্যবহারের কারণ | | | |
| 2 | আপনার জানা ব্রাউজার | | | |
| 3 | যেসব জিনিস একটি VPN লুকিয়ে রাখতে পারে | | | |
| 4 | গোপনীয়তার সঙ্গে সম্পর্কিত শব্দ | | | |
| 5 | এই ওয়ার্কশিটের যে শব্দগুলো আপনি মনে রাখতে চান | | | |
| 6 | একটি ওয়েবসাইট আপনার IP থেকে যা যা অনুমান করতে পারে | | | |
| 7 | একটি IP অ্যাড্রেসে থাকা সংখ্যা বা চিহ্ন | | | |
| 8 | VPN নিয়ে প্রচলিত ভুল ধারণা | | | |
| 9 | আপনার জানা VPN সার্ভিস | | | |
| 10 | আপনার ইন্টারনেট প্রদানকারী যা যা দেখতে পায় | | | |
| 11 | একজন ভালো VPN প্রদানকারীর প্রতিশ্রুতি | | | |
| 12 | যেসব জিনিস আপনার আসল IP ফাঁস করতে পারে | | | |
| 13 | আপনার অবস্থান লুকানোর কারণ | | | |
| 14 | আপনার IP অ্যাড্রেস লুকানোর উপায় | | | |
| 15 | যেসব ডিভাইসে VPN ব্যবহার করা যায় | | | |

# চেকপয়েন্ট 8: VPN কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

### সারাহ (ক্যাফের শিক্ষার্থী)

👱 "হ্যালো! আমি Coffee & Bytes-এ বসে আছি। এখানে 'Free_Wi-Fi_No_Password' নামে একটি অনিরাপদ পাবলিক নেটওয়ার্ক আছে। আমি আমার স্কুলের ইমেইলে লগ ইন করে অ্যাসাইনমেন্ট আপলোড করতে চাই, কিন্তু হ্যাকারদের নিয়ে চিন্তিত। VPN ছাড়া এই নেটওয়ার্ক ব্যবহার করলে কী কী ঝুঁকি আছে, আর VPN কীভাবে আমার ডেটা সুরক্ষিত করে?"

### অ্যালেক্স (ভ্রমণকারী শিক্ষার্থী)

👱 "ইশ! আমি একটি প্রকল্পের জন্য বিদেশে ভ্রমণ করছি এবং আমার নিজের দেশের একটি সার্ভারে হোস্ট করা জীববিজ্ঞানের ডকুমেন্টারি দেখার চেষ্টা করছি। কিন্তু সাইট বলছে 'এই ভিডিও আপনার বর্তমান অবস্থানে উপলব্ধ নয়।' আমি কেন ব্লক হচ্ছি, আর VPN কীভাবে আমাকে এটি দেখতে সাহায্য করতে পারে?"

# চেকপয়েন্ট 9: সংকেতবার্তা ডিকোড করুন

আপনার IP মাস্কিং প্রশিক্ষণ সম্পন্ন করতে ডিজিটাল চিহ্ন লুকানো সম্পর্কিত এই গোপন বার্তাটি ডিক্রিপ্ট করুন।

**অক্ষর-থেকে-সংখ্যা এনক্রিপশন কী**

অ=1 আ=2 ই=3 ঈ=4 উ=5 ঊ=6 ঋ=7 এ=8 ঐ=9 ও=10 ঔ=11 ক=12
খ=13 গ=14 ঘ=15 ঙ=16 চ=17 ছ=18 জ=19 ঝ=20 ঞ=21 ট=22 ঠ=23 ড=24
ঢ=25 ণ=26 ত=27 থ=28 দ=29 ধ=30 ন=31 প=32 ফ=33 ব=34 ভ=35 ম=36
য=37 র=38 ল=39 শ=40 ষ=41 স=42 হ=43 ৎ=44 া=45 ি=46 ী=47 ু=48
ূ=49 ৃ=50 ে=51 ৈ=52 ো=53 ৌ=54 ং=55 ঃ=56 ঁ=57 ্=58 ়=59

| 39 | 48 | 12 | 45 | 31 | | 2 | 32 | 31 | 45 | 38 | | 23 | 46 | 12 | 45 | 31 | 45 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | |

| 14 | 53 | 32 | 31 | | 34 | 58 | 37 | 34 | 42 | 58 | 28 | 45 | 37 | 59 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | |

## ডিকোড করা বার্তা:

পরামর্শ: প্রতিটি সংখ্যা বর্ণমালায় সেই অক্ষরের অবস্থান বোঝায় (যেমন 1 = অ, 2 = আ, 63 = ়)।

# চেকপয়েন্ট 10: মৌলিক VPN FAQ (অংশ A)

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ব্যবহার সম্পর্কে সম্ভাব্য গ্রাহকদের সবচেয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

### Q1: VPN কী এবং এটি কীভাবে কাজ করে?

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN) আপনার ইন্টারনেট সংযোগ এনক্রিপ্ট করে এবং ট্রাফিককে একটি নিরাপদ রিমোট সার্ভারের মধ্য দিয়ে পাঠায়। এতে আপনার পাবলিক IP অ্যাড্রেস আড়াল হয় এবং VPN টানেল দিয়ে যাওয়া ট্রাফিক সম্পর্কে স্থানীয় নেটওয়ার্ক পর্যবেক্ষক ও আপনার ISP কী দেখতে পারে, তা সীমিত হয়।

### Q2: আমি কেন VPN ব্যবহার করব?

VPN আপনার ডিজিটাল গোপনীয়তা সুরক্ষা করে, পাবলিক Wi-Fi নেটওয়ার্কে (যেমন ক্যাফে বা বিমানবন্দরে) আপনার সংযোগ নিরাপদ রাখে, ISP এনক্রিপ্টেড ট্রাফিকের ধরন শনাক্ত করতে না পারলে কার্যকলাপভিত্তিক থ্রটলিং কমাতে পারে, ভৌগোলিক নিষেধাজ্ঞা এড়িয়ে বৈশ্বিক কনটেন্টে প্রবেশের সুযোগ দেয় এবং রিমোট কাজের রিসোর্স সুরক্ষিত রাখতে সহায়তা করে।

### Q3: VPN কি আমাকে অনলাইনে সম্পূর্ণ বেনামি করে দেয়?

না। VPN আপনার IP ঠিকানা লুকায় ও ট্রাফিক এনক্রিপ্ট করলেও ব্রাউজার কুকি, সক্রিয় অ্যাকাউন্ট (যেমন Google বা Facebook), ব্রাউজার ফিঙ্গারপ্রিন্টিং, অথবা আপনার VPN প্রোভাইডার ডেটা লগ করলে আপনাকে তবুও ট্র্যাক করা যেতে পারে।

### Q4: ওয়েব প্রক্সি কি আমার IP অ্যাড্রেস লুকায়?

হ্যাঁ, তবে শুধু এর মধ্য দিয়ে পাঠানো ট্রাফিকের ক্ষেত্রে, সাধারণত আপনার ব্রাউজারের। বেশিরভাগ ওয়েব প্রক্সি আপনার ডেটা এনক্রিপ্ট করে না, তাই আপনার ISP বা নেটওয়ার্ক অপারেটর এখনও দেখতে পারে আপনি কী পাঠান ও গ্রহণ করেন।

### Q5: আমার IP লুকানো কি বৈধ?

অনেক দেশে হ্যাঁ, তবে কিছু দেশ IP ঠিকানা লুকাতে ব্যবহৃত VPN ও অন্যান্য সরঞ্জাম সীমিত বা নিষিদ্ধ করে। IP লুকালে কোনো অবৈধ কাজ বৈধ হয়ে যায় না, তাই ব্যবহারের আগে স্থানীয় আইন দেখে নিন।

# চেকপয়েন্ট 10: মৌলিক VPN FAQ (অংশ B)

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ব্যবহার সম্পর্কে সম্ভাব্য গ্রাহকদের সবচেয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

### Q6: Tor কি আমার IP লুকায়?

হ্যাঁ। Tor আপনার ট্রাফিক তিনটি স্বেচ্ছাসেবী রিলের (গার্ড, মিডল ও এক্সিট) মধ্য দিয়ে পাঠায়, ফলে ওয়েবসাইট এক্সিট রিলের ঠিকানা দেখে, এবং কোনো একটি রিলই একসঙ্গে জানে না আপনি কে এবং কোথায় যাচ্ছেন। [1]

### Q7: আমার IP কী প্রকাশ করে?

আপনার পাবলিক IP সাধারণত আপনার ISP এবং আনুমানিক অবস্থান, যেমন আপনার দেশ বা শহর, প্রকাশ করে। সাইটগুলো এটি ব্যবহার করে আপনার ভিজিট একসঙ্গে যুক্ত করতে এবং ভৌগোলিক ব্লক প্রয়োগ করতেও পারে।

### Q8: এটি লুকানো আছে কি না, আমি কীভাবে তা পরীক্ষা করব?

আপনার VPN-এ সংযুক্ত হয়ে একটি IP-যাচাই সাইটে যান এবং DNS ও WebRTC লিক পরীক্ষা চালান। দেখানো IP ও DNS সার্ভার VPN-এর হওয়া উচিত, আপনার ISP-র নয়। আপনার আসল IP দেখা গেলে লিক সুরক্ষা চালু করুন।

### Q9: আমি কি আমার ফোন ও স্মার্ট টিভিতে VPN ব্যবহার করতে পারি?

হ্যাঁ। আধুনিক VPN প্রদানকারীরা iOS, Android, macOS, Windows, Linux ও স্মার্ট টিভির জন্য ডেডিকেটেড অ্যাপ দেয়, পাশাপাশি আপনার হোম নেটওয়ার্কের সব ডিভাইস সুরক্ষিত করতে রাউটার সেটআপও দেয়।

### Q10: কিল সুইচ কী?

কিল সুইচ এমন একটি নিরাপত্তা ফিচার, যা VPN সংযোগ বিচ্ছিন্ন হলে আপনার ডিভাইসকে স্বয়ংক্রিয়ভাবে ইন্টারনেট থেকে বিচ্ছিন্ন করে দেয়। এতে আপনার এনক্রিপশনবিহীন ডেটা বা প্রকৃত IP অ্যাড্রেস ফাঁস হওয়া ঠেকানো যায়।

# চেকপয়েন্ট 10: উন্নত VPN FAQ (অংশ C)

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ও নিরাপদ টানেলিং প্রোটোকলের প্রযুক্তিগত ও কাঠামোগত দিক অন্বেষণ করুন।

### Q1: IP ঠিকানা লুকানোর পরও ওয়েবসাইট আমাকে ট্র্যাক করতে পারে কেন?

আপনার IP লুকালে ব্রাউজার ফিঙ্গারপ্রিন্টিং বন্ধ হয় না। ট্র্যাকাররা আপনার স্ক্রিন রেজোলিউশন, ইনস্টল করা ফন্ট ও ব্রাউজার সেটিংসের মতো তথ্য মিলিয়ে একটি শনাক্তকারী তৈরি করতে পারে, এবং কুকি বা সাইন-ইন করা অ্যাকাউন্টও আপনাকে শনাক্ত করতে পারে, তাই একটি গোপনীয়তা-কেন্দ্রিক ব্রাউজারও ব্যবহার করুন। [3]

### Q2: ডাবল VPN বা Multi-Hop রাউটিং কী?

মাল্টি-হপ আপনার ট্রাফিককে পরপর দুই বা ততোধিক VPN সার্ভারের মধ্য দিয়ে রুট করে। এটি দ্বিতীয় একটি এনক্রিপশন স্তর যোগ করে এবং একটি সার্ভার আপস হলে দ্বিতীয় হপ থেকে আপনার আসল IP ঠিকানা লুকিয়ে রাখতে সাহায্য করে।

### Q3: WebRTC লিকিং কী এবং VPN কীভাবে তা প্রতিরোধ করে?

WebRTC একটি ব্রাউজার প্রোটোকল, যা VPN সক্রিয় থাকলেও আপনার আসল লোকাল ও পাবলিক IP অ্যাড্রেস প্রকাশ করে দিতে পারে। প্রিমিয়াম VPN তাদের ডেস্কটপ/মোবাইল অ্যাপ ও ব্রাউজার এক্সটেনশনে WebRTC অনুরোধ ব্লক বা স্পুফ করে।

### Q4: IPv6 ট্রাফিক কি আমার আসল IP অ্যাড্রেস ফাঁস করতে পারে?

হ্যাঁ, যদি আপনার VPN কেবল IPv4 টানেল করে। তখন আপনার ডিভাইস IPv6 ট্রাফিক টানেলের বাইরে পাঠাতে পারে, ফলে ISP-র বরাদ্দ করা ঠিকানা প্রকাশ পায়। IPv6 টানেল বা ব্লক করে এমন VPN ব্যবহার করুন এবং IPv6 লিক টেস্ট দিয়ে নিশ্চিত হয়ে নিন।

### Q5: অবফাসকেশন কীভাবে VPN ব্লক এড়িয়ে যায়?

অবফাসকেশন (বা "স্টিলথ VPN") VPN ট্রাফিকের প্যাকেটকে সাধারণ HTTPS ওয়েব ট্রাফিকের (পোর্ট 443) মতো দেখায়। এটি সরকার বা স্কুল/অফিস নেটওয়ার্কের VPN ব্লক করতে ব্যবহৃত ডিপ প্যাকেট ইন্সপেকশন (DPI) পার হতে সাহায্য করে।

# চেকপয়েন্ট 10: উন্নত VPN FAQ (অংশ D)

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ও নিরাপদ টানেলিং প্রোটোকলের প্রযুক্তিগত ও কাঠামোগত দিক অন্বেষণ করুন।

### Q6: স্প্লিট টানেলিং কি আমার আসল IP অ্যাড্রেস প্রকাশ করে?

হ্যাঁ, আপনি যে অ্যাপগুলো বাদ দেন সেগুলোর ক্ষেত্রে। টানেলের বাইরে পাঠানো ট্রাফিক আপনার আসল IP ব্যবহার করে, এবং RFC 8828 উল্লেখ করে যে ব্রাউজার সীমিত না করলে স্প্লিট-টানেল VPN-এর নিচেও WebRTC ISP-র ঠিকানা প্রকাশ করতে পারে। [2]

### Q7: শেয়ার্ড IP অ্যাড্রেস কী এবং এটি গোপনীয়তায় কীভাবে সাহায্য করে?

শেয়ার্ড IP থাকলে অনেক VPN ব্যবহারকারী একই সময়ে একই অ্যাড্রেস নিয়ে অনলাইনে দেখা যায়। ফলে শুধু আপনার ব্যবহৃত ডেডিকেটেড IP-র তুলনায় কোনো ওয়েবসাইটের পক্ষে একটি একক ভিজিটকে আপনার সঙ্গে যুক্ত করা অনেক কঠিন হয়।

### Q8: আমার IP লুকাতে VPN ব্যবহার করছি, আমার ISP কি তা দেখতে পায়?

সাধারণত হ্যাঁ। আপনার ISP দেখতে পারে যে আপনি একটি VPN সার্ভারের IP ঠিকানায় সংযুক্ত হচ্ছেন, কখন সংযুক্ত হচ্ছেন এবং কত ডেটা পাঠাচ্ছেন, কিন্তু আপনি কোন ওয়েবসাইট দেখছেন বা এনক্রিপ্টেড টানেলের ভেতরের কনটেন্ট দেখতে পারে না।

### Q9: DNS লিক সুরক্ষা কী?

DNS লিক সুরক্ষা আপনার ডিভাইসকে ওয়েবসাইট লুকআপ কোয়েরি (DNS কোয়েরি) আপনার ISP-র সার্ভারের বদলে VPN-এর প্রাইভেট, এনক্রিপ্টেড DNS সার্ভারের মাধ্যমে পাঠাতে বাধ্য করে। এতে আপনার ISP আপনি কোন সাইটে যান তা ট্র্যাক করতে পারে না।

### Q10: IP লুকাতে প্রক্সি না VPN, কোনটি ভালো?

সাধারণত VPN-ই ভালো। এটি ডিভাইসের প্রতিটি অ্যাপের জন্য আপনার IP লুকায় ও ট্রাফিক এনক্রিপ্ট করে, অন্যদিকে ওয়েব প্রক্সি সাধারণত শুধু ব্রাউজারকে কভার করে এবং প্রায়ই কোনো এনক্রিপশন যোগ করে না।

# অংশ 11: 10টি আকর্ষণীয় VPN তথ্য ও বাস্তব অন্তর্দৃষ্টি

VPN-এর ইতিহাস, বাজার ও প্রযুক্তি সম্পর্কে এই অত্যন্ত মূল্যবান বাস্তব তথ্য ও অন্তর্দৃষ্টিগুলো দেখে নিন।

### 1. প্রথম VPN প্রটোকল

PPTP (Point-to-Point Tunneling Protocol) 1990-এর দশকে Microsoft-নেতৃত্বাধীন একটি গ্রুপের তৈরি প্রাথমিক VPN প্রোটোকল, যা এখন অনিরাপদ বলে বিবেচিত, তাই আধুনিক VPN WireGuard বা OpenVPN ব্যবহার করে।

### 2. ফিঙ্গারপ্রিন্টিং

আপনার IP লুকালে ব্রাউজার ফিঙ্গারপ্রিন্টিং বন্ধ হয় না, যা স্ক্রিন রেজোলিউশন ও ইনস্টল করা ফন্টের মতো তথ্য থেকে আপনাকে শনাক্ত করতে পারে। [3]

### 3. WireGuard বিপ্লব

WireGuard-এর কোডবেস অত্যন্ত সুবিন্যস্ত ও দক্ষতার জন্য নকশা করা, ফলে প্রচলিত প্রোটোকলের চেয়ে নিরাপত্তা দুর্বলতার জন্য নিরীক্ষা করা সহজ।

### 4. WebRTC ঠিকানা প্রকাশ

RFC 8828 সতর্ক করে যে ব্রাউজার সীমাবদ্ধ না করলে WebRTC একটি VPN-এর পাবলিক অ্যাড্রেস এবং যে ISP-র ওপর VPN চলছে তার অ্যাড্রেস, দুটিই খুঁজে পেতে পারে। [2]

### 5. 5-Eyes জোটের উৎস

US, UK, Canada, Australia ও New Zealand-এর Five Eyes গোয়েন্দা অংশীদারির সূচনা দ্বিতীয় বিশ্বযুদ্ধের সময়ে মিত্রদের মধ্যকার সিগন্যাল-ইন্টেলিজেন্স সহযোগিতা থেকে।

### 6. ডিপ প্যাকেট ইন্সপেকশন

উন্নত ফায়ারওয়াল নেটওয়ার্ক প্যাকেটের মেটাডেটা বিশ্লেষণ ও স্ট্যান্ডার্ড VPN সংযোগের বৈশিষ্ট্য ব্লক করতে ডিপ প্যাকেট ইন্সপেকশন (DPI) প্রয়োগ করে।

### 7. টর সার্কিট পুনর্ব্যবহার

Tor প্রায় দশ মিনিট একই সার্কিট ব্যবহার করে, তারপর নতুন একটি তৈরি করে, যা আপনার ব্রাউজিং কার্যকলাপ একসঙ্গে যুক্ত করা কঠিন করে তোলে। [1]

### 8. বিকেন্দ্রীকৃত VPN

বিকেন্দ্রীভূত VPN (dVPN) ট্রাফিককে পিয়ার-চালিত নোডের নেটওয়ার্কে ছড়িয়ে দেয়, ফলে একক কেন্দ্রীভূত প্রোভাইডারের ওপর নির্ভরতা কমে।

### 9. টর বনাম VPN অজ্ঞাতপরিচয়

VPN একটিমাত্র প্রদানকারীর মধ্য দিয়ে ট্রাফিক টানেল করে, আর Tor (দ্য অনিয়ন রাউটার) গোপনীয়তা সর্বোচ্চ করতে তিনটি স্বেচ্ছাসেবী রিলের (গার্ড, মিডল, এক্সিট) মধ্য দিয়ে ট্রাফিক পাঠায়। [1]

### 10. প্রক্সি বনাম VPN টানেল

ওয়েব প্রক্সি আপনার ব্রাউজার ট্রাফিকের জন্য কোনো সাইট যে IP অ্যাড্রেস দেখে তা বদলে দেয়, কিন্তু VPN-এর মতো নয়, এটি সাধারণত সেই ট্রাফিক এনক্রিপ্ট করে না বা আপনার ডিভাইসের অন্য অ্যাপকে কভার করে না। [5]

# প্রযুক্তিগত তথ্যসূত্র ও উৎস

এই ওয়ার্কশিটে ব্যবহৃত উদ্ধৃত প্রকাশনা, ক্রিপ্টোগ্রাফিক স্পেসিফিকেশন ও অফিসিয়াল নথির মান।

## গবেষণামূলক ও শিল্পক্ষেত্রের তথ্যসূত্র

[1] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.
https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.
https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

# উত্তরমালা: IP ঠিকানা লুকানো, অবস্থান গোপন করা, প্রক্সি, Tor এবং DNS/WebRTC লিক রোধ

## 1 প্রশ্ন 1

**সঠিক উত্তর: B**

### শিক্ষণ নোট

আপনার ভিজিট করা ওয়েবসাইটগুলোর কাছে একটি ডিভাইসের পাবলিক IP অ্যাড্রেস কী প্রকাশ করে? → আপনার আনুমানিক অবস্থান এবং ISP-র নাম

## 2 VPN সিস্টেম এনক্রিপশন

ল্যাটেন্সি

**সঠিক উত্তর: C**

### শিক্ষণ নোট

যেসব প্রক্সি শুধু ব্রাউজার ট্রাফিক পুনঃনির্দেশ করে তাদের বিপরীতে VPN সিস্টেম জুড়ে একটি এনক্রিপ্টেড টানেল তৈরি করে, যা ব্যাকগ্রাউন্ড অ্যাপ্লিকেশন, গেম ও OS কোয়েরি সুরক্ষিত রাখে। সূত্র: Tor Project Relays, W3C WebRTC API।

## 3 প্রক্সিতে এনক্রিপশনের অভাব

ওয়াই-ফাই নিরাপত্তা

**সঠিক উত্তর: A**

### শিক্ষণ নোট

ওয়েব প্রক্সি শুধু ব্রাউজারের ট্রাফিক ফরওয়ার্ড করে, প্যাকেট পেলোড এনক্রিপ্ট করে না, অর্থাৎ আপনার নেটওয়ার্ক অপারেটর বা ISP এখনও আপনার কনটেন্ট ট্রাফিক শনাক্ত করতে পারে। সূত্র: IETF Proxy Vulnerabilities।

## 4 প্রশ্ন 4

**সঠিক উত্তর: B**

### শিক্ষণ নোট

Tor নেটওয়ার্ক ব্যবহারকারীদের উচ্চ বেনামিত্ব কীভাবে দেয়? → স্বেচ্ছাসেবীদের চালানো তিনটি রিলের মধ্য দিয়ে ট্রাফিক পাঠিয়ে

## 5 DNS টানেল লিক

গোপনীয়তা

**সঠিক উত্তর: B**

### শিক্ষণ নোট

ডোমেইন নেম রেজোলিউশনের অনুরোধ VPN টানেল পাশ কাটিয়ে সরাসরি আপনার ISP-র রিজলভারে গেলে DNS লিক ঘটে, ফলে দেখা ডোমেইনের রেকর্ড প্রকাশ পেয়ে যায়। সূত্র: DNSSEC Tunnel Testing, EFF Tracking Evasion।

## উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

### 6 প্রক্সির সীমাবদ্ধতার বিবরণ IP মাস্কিং

সঠিক উত্তর: মিথ্যা

#### শিক্ষণ নোট

প্রক্সি অ্যাপ্লিকেশন স্তরে কাজ করে এবং VPN টানেলের মতো সিস্টেম-ব্যাপী নেটওয়ার্ক ড্রাইভার সংযোজন এতে নেই। তথ্যসূত্র: IETF Proxy Vulnerabilities।

### 7 প্রশ্ন 7

সঠিক উত্তর: সত্য

#### শিক্ষণ নোট

স্তরভিত্তিক এনক্রিপশনসহ তিনটি স্বেচ্ছাসেবী রিলের মধ্য দিয়ে ট্রাফিক পাঠালে লেটেন্সি বাড়ে, তাই Tor সাধারণত সরাসরি সংযোগের চেয়ে ধীর।

### 8 প্রশ্ন 8

সঠিক উত্তর: সত্য

#### শিক্ষণ নোট

WebRTC লোকাল অ্যাড্রেস প্রকাশ করতে পারে, এবং কিছু VPN সেটআপে টানেলের নিচে ISP-র দেওয়া পাবলিক IP-ও প্রকাশ করতে পারে (RFC 8828)।

### 9 প্রশ্ন 9

সঠিক উত্তর: সত্য

#### শিক্ষণ নোট

DNS বা WebRTC ফাঁস না থাকলে ISP শুধু VPN সার্ভারের দিকে যাওয়া এনক্রিপ্ট করা ট্রাফিক দেখে, আপনি কোন সাইটে যান তা নয়।

### 10 ফিঙ্গারপ্রিন্টিংয়ের সীমা নো-লগ

সঠিক উত্তর: মিথ্যা

#### শিক্ষণ নোট

ফিঙ্গারপ্রিন্টিং ডিভাইস কনফিগারেশন মেট্রিক (স্ক্রিন রেজোলিউশন, ফন্ট, প্লাগইন) লক্ষ্য করে, যা IP লুকানো থাকলেও দৃশ্যমান থাকে। তথ্যসূত্র: EFF Tracking Evasion।

# শব্দভাণ্ডারের উত্তরমালা ও মূল্যায়ন রুব্রিক

**শিক্ষকের মূল্যায়ন রুব্রিক: প্রতিটি সঠিক মিলের জন্য (মোট ৪ নম্বর) এবং প্রসঙ্গ পরিভাষার জন্য (মোট 6 নম্বর) 1 নম্বর দিন।**

## চেকপয়েন্ট 4: উত্তর – ধারণা মিলান

| | | | |
|---|---|---|---|
| D 1. IP ঠিকানা | A 2. VPN টানেল | B 3. Tor নেটওয়ার্ক | E 4. ওয়েব প্রক্সি |
| G 5. DNS লিক | H 6. WebRTC API | C 7. অবস্থান আড়াল করা | F 8. ISP ট্র্যাকিং |

## চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

| | | | |
|---|---|---|---|
| 1 ডিএনএস লিক | 2 WebRTC | 3 প্রক্সি | 4 টর |
| 5 আইপি ঠিকানা | 6 লোকেশন | | |

## চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

| | | | |
|---|---|---|---|
| 1 D – ওয়েবআরটিসি | 2 G – এনক্রিপশন | 3 F – লগইন | 4 A – আইপিঅ্যাড্রেস |
| 5 C – ওয়েবপ্রক্সি | 6 H – অ্যাকাউন্ট | 7 E – আইএসপিট্র্যাকিং | 8 B – ভিপিএনটানেল |

### শিক্ষকদের জন্য আলোচনা নোট

**মূল পরিভাষা:**
যাচাই করুন শিক্ষার্থীরা IP ঠিকানা, VPN টানেল ও Tor নেটওয়ার্ক নিজের ভাষায় ব্যাখ্যা করতে এবং প্রতিটির একটি উদাহরণ দিতে পারে কি না।

**কেস স্টাডি:**
শিক্ষার্থীদের বলুন তারা যেন মতামতের বদলে ওয়ার্কশিটের তথ্যের ভিত্তিতে সুপারিশ করে।

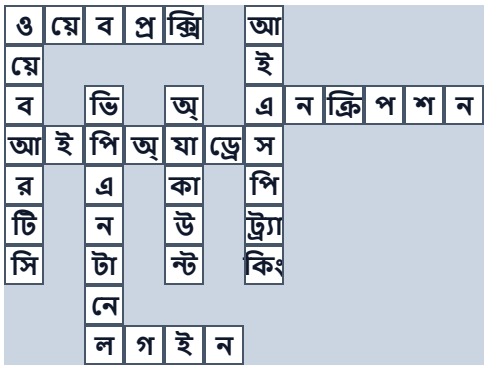
**উৎস মূল্যায়ন:**
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

# ধাঁধার উত্তরমালা ও শিক্ষকের নোট

## শব্দ খোঁজার সমাধান

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ক | সি | দ | ঠ | হ | সা | শ | মে | দে | রা | কি | ঋ | তে | না | নে |
| ছ | য | ক্সি | প | উ | অ | উ | ঋ | আ | মা | বা | য | ফ | বা | ম |
| দে | তি | প্র | ভ | ঘ | রে | ষ | ফ | ঘ | ই | দ | হ | স | ভ | রি |
| মি | ঢ | ব | ন | শ | প | ক্রি | ন | এ | ষ | এ | ষ | রি | সি | না |
| তি | তা | য়ে | ড | ঊ | আ | নি | রা | কি | থ | সে | স | ঊ | লি | গ |
| সি | নি | ও | জা | পি | ই | ঋ | ভি | জি | ন্ট | লি | ট | পি | ভ | ণ |
| টি | জে | গ | স | ঘ | পি | রে | দি | পি | মি | উ | ঋ | পা | ট্র্যা | উ |
| র | অ | জে | কা | গ | অ্ | ম | আ | ঘ | এ | কি | কা | ঘ | ঝ | কিং |
| আ | ণ | ধ | গ | সি | যা | রি | শ | ছ | দ | ন | সে | যা | জি | নি |
| ব | ঝ | রে | পে | জ | ড্রে | ল | আ | আ | রে | মা | টা | স | অ্ | মে |
| য়ে | তি | দে | রি | ফ | স | গ | সি | তি | সে | খ | স | নে | বে | উ |
| ও | ট | সে | দি | দা | প | ই | আ | সি | জে | বি | বি | য | ল | ড |
| দ | ষ | সা | ফ | ল | ল | ন | তা | কে | ণ | রা | রি | ণ | জে | ই |
| কে | পে | ঠ | পি | ঊ | বে | সে | বে | উ | ণ | ল | জে | ঢ | ফ | কি |
| মে | কা | দা | ঋ | ল | জে | বে | ঠ | বি | কে | লে | পা | ম | পি | মি |

## ক্রসওয়ার্ডের সমাধান




## ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

### পাশাপাশি

**1 পাশাপাশি: ওয়েবপ্রক্সি** সিস্টেম-এনক্রিপশন ছাড়া অ্যাপ্লিকেশন স্তরে ব্রাউজার ট্র্যাফিক পুনঃনির্দেশ করে (5 অক্ষর)

**5 পাশাপাশি: এনক্রিপশন** তথ্যকে অন্যের কাছে অপাঠ্য কোডে রূপান্তরের পদ্ধতি (6 অক্ষর)

**6 পাশাপাশি: আইপিঅ্যাড্রেস** ইন্টারনেটে ডিভাইসের ইন্টারফেস শনাক্তকারী অনন্য সংখ্যাসূচক লেবেল (7 অক্ষর)

**7 পাশাপাশি: লগইন** নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4 অক্ষর)

### উপর-নিচ

**1 উপর-নিচ: ওয়েবআরটিসি** ভয়েস ও ভিডিওর ব্রাউজার ফিচার, যা টানেল এড়িয়ে আসল আইপি ঠিকানা ফাঁস করতে পারে (7 অক্ষর)

**2 উপর-নিচ: আইএসপিট্র্যাকিং** আপনার টেলিকম প্রদানকারীর অনএনক্রিপ্টেড ইন্টারনেট ট্র্যাফিকের গন্তব্য লগ করা (7 অক্ষর)

**3 উপর-নিচ: ভিপিএনটানেল** ডিভাইসের সব ট্র্যাফিক এনক্রিপ্ট করে ভিপিএন সার্ভার দিয়ে পাঠায় (7 অক্ষর)

**4 উপর-নিচ: অ্যাকাউন্ট** সেবা ব্যবহারের জন্য তৈরি ব্যক্তিগত নিবন্ধন (5 অক্ষর)

# এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

শব্দভাণ্ডার অক্ষর-সাজানো কার্যক্রম ও Secret Cipher Challenge-এর মূল্যায়ন উত্তরমালা।

## শব্দ সাজানোর উত্তরমালা

1. অ্যাড্রেআযাসপিই — **আইপিঅ্যাড্রেস**
2. ওক্সিপ্রবয়ে — **ওয়েবপ্রক্সি**
3. সআপিকিংএট্র্যাই — **আইএসপিট্র্যাকিং**
4. নপক্রিশএন — **এনক্রিপশন**
5. টালনএভিনেপি — **ভিপিএনটানেল**
6. টিবরওআসিয়ে — **ওয়েবআরটিসি**
7. ইলনগ — **লগইন**
8. ন্টঅ্কাউযা — **অ্যাকাউন্ট**

### গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

**"লুকান আপনার ঠিকানা গোপন ব্যবস্থায়"**

# কেস স্টাডির উত্তর

## A পরিস্থিতি A: পাবলিক নেটওয়ার্ক নিরাপত্তা

স্নিফিং ও এনক্রিপশন | সারাহর উভয়সংকট

### মূল্যায়ন নির্দেশিকা

**শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:**

- ঝুঁকি: প্যাকেট স্নিফিং, ডেটা ইন্টারসেপশন এবং ম্যান-ইন-দ্য-মিডল আক্রমণ। একই ক্যাফের নেটওয়ার্কে থাকা কেউ তার লগইনের তথ্য বা হোমওয়ার্ক ফাইল ধরে ফেলতে পারে।
- VPN সুরক্ষা: নেটওয়ার্ক প্যাকেটের পেলোড এনক্রিপ্ট করে, ফলে VPN সঠিকভাবে কনফিগার করা থাকলে আটকানো টানেল ট্রাফিক নিষ্ক্রিয় স্থানীয়-নেটওয়ার্ক আড়িপাতাকারীদের কাছে অপাঠ্য হয়ে যায়।

## B পরিস্থিতি B: অবরুদ্ধ রিসোর্সে প্রবেশ

জিও-ব্লকিং ও IP | অ্যালেক্সের দ্বিধা

### মূল্যায়ন নির্দেশিকা

**শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:**

- কেন ব্লক হয়েছে: স্ট্রিমিং হোস্ট জিও-ব্লকিং ব্যবহার করে, যা ভ্রমণকারী তার স্থানীয় IP অ্যাড্রেসকে তার ভৌত দেশের সঙ্গে মিলিয়ে ভৌগোলিক লাইসেন্সিংয়ের ভিত্তিতে ব্লক করে।
- VPN কীভাবে সাহায্য করে: নিজ দেশের সার্ভারের মাধ্যমে ট্রাফিক পাঠিয়ে তার আসল অবস্থান লুকানো। সাইটটি নিজ দেশের IP দেখে, ফলে অ্যাক্সেস পাওয়া যায়।