یونٹ 4 ڈیٹا اور رازداری کا معاملہ
(Data and Privacy)

مختصر تعارف (Short Introduction)

ڈیٹا کی منتقلی ہم پچھلے باب میں بیان کر چکے ہیں۔ اس باب میں ہم ڈیٹا کی محفوظ منتقلی کے بارے میں جانیں گے۔ ڈیٹا منتقل کرنے سے پہلے اسے نا پڑھی جا سکنے والی شکل میں تبدیل کر دیا جاتا ہے اور جب وہ اپنی منزل پر پہنچ جاتا ہے تو دوبارہ پڑھی جانے والی شکل میں تبدیل کر دیا جاتا ہے۔ اس باب میں ڈیٹا کی اس قسم کی محفوظ منتقلی کے طریقے بتائے جائیں گے نیٹ ورک سے منسلک ہونے کے بعد ایک کمپیوٹر دوسرے کمپیوٹروں تک رسائی حاصل کر سکتا ہے۔ اس باب میں حساس ڈیٹا کو نیٹ ورک پر منتقل کرنے کے حفاظتی اقدامات بیان کیے جائیں گے۔

حاصلاتِ تعلم (Students Learning Outcomes)

-1 سیکورٹی سے متعلق اخلاقی مسائل:

- ڈیٹا کی سیکورٹی سے متعلق اخلاقی مسائل کو سمجھنا۔
- دوسروں کی رازداری کی حفاظت کو اپنی ذمہ داری سمجھنا۔

-2 ڈیٹا رازداری کی اہمیت:

- ڈیٹا کے بڑے مجموعے سے رازداری کے خدشات پیدا ہوتے ہیں ان کی وضاحت کرنا۔
- ذاتی رازداری اور حفاظتی خدشات جو کہ کمپیوٹنگ سسٹم کو استعمال کرنے سے پیدا ہوتے ہیں ان کا تجزیہ کرنا۔

-3 سادہ خفیہ کاری:

- وضاحت کریں انٹرنیٹ پر روزمرہ کے کام کرنے کے لیے خفیہ کاری کی کیوں ضرورت ہے؟
- سیزر سائیفر (Caeser Cipher) وجیٹ (Widget) کا استعمال کرتے ہوئے سیزر سائیفر کے استعمال سے بنائے خفیہ پیغام کو توڑنا۔
- فریکوئینسی تجزیہ (Frequency Analysis) کا استعمال کرتے ہوئے بے ترتیب متبادل (Random Substitution) کے ساتھ خفیہ کردہ پیغام کو توڑنا۔
- سبسٹی ٹیوشن سائیفر (Substitution Ciphers) کی کمزوریاں اور حفاظتی خرابیوں کی وضاحت کرنا۔

-4 کیز (Keys) اور پاس ورڈ (Password) کے ساتھ خفیہ کاری:

- کرپٹوگرافی کی (Cryptographic Key) اور پاس ورڈ (Password) کے درمیان تعلق بیان کرنا۔
- وضاحت سے بیان کریں کہ وہ کیا ہے جو ایک کی (Key) کو توڑنے میں مشکل بناتا ہے۔
- کسی بھی کمپیوٹر ٹول کو استعمال کرتے ہوئے مضبوط اور کمزور پاس ورڈ (Password) کی وضاحت کریں۔
- اچھے پاس ورڈ کی خوبیاں

-5 سائبر (Cyber) جرم:

- (Phishing) فشنگ حملے کی خوبیاں بیان کرنا۔
- (Denial of Service) DOS حملہ کس طرح ہوتا ہے بیان کرنا۔

for notes, past papers, free test sessions and guess papers visit taleemcity.com

سوال1: ڈیٹا اور رازداری کا تعارف بیان کریں۔

جواب: **ڈیٹا اور رازداری کا تعارف (Introduction about Data and Privacy)**

آج کل تقریباً ہر عمر کے لوگ کمپیوٹر کا استعمال کرتے ہیں۔ ای میل اکاؤنٹ بناتے ہوئے، آن لائن خریداری کرتے، ہسپتال کا دورہ کرتے ہوئے اور سکول میں داخلہ لیتے وقت ہم اپنی ذاتی معلومات کمپیوٹر میں اندراج کرتے یا کرواتے ہیں۔ ہم یہ خیال کرتے ہیں کہ ہماری فراہم کردہ معلومات کسی کو نہیں بتائی جائیں گی۔ ضرر پہنچانے (ڈیٹا چرانے) والے صارفین سے ڈیٹا کی حفاظت کرنا، ڈیٹا یا معلومات کی رازداری کہلاتی ہے۔

سوال2: ڈیٹا سکیورٹی سے متعلق اخلاقی مسائل کیا ہوتے ہیں؟

جواب: **ڈیٹا سکیورٹی سے متعلق اخلاقی مسائل (Ethical Issues Related to Security)**

تمام حفاظتی نظام کی بنیاد اخلاقی اصولوں پر قائم ہے۔ اگر ہمارے پاس دوسروں کا ڈیٹا ہے تو یہ ہماری اخلاقی ذمہ داری ہے کہ ہم اسے محفوظ رکھیں۔ ڈیٹا سکیورٹی کے چند مسائل درج ذیل ہیں:۔

(i)	رازداری اور پوشیدگی	(ii)	دھوکہ دہی اور غلط استعمال	(iii)	پیٹنٹ
(iv)	کاپی رائٹ	(v)	تجارتی راز	(vi)	تخریب کاری

سوال3: ڈیٹا سکیورٹی سے متعلق اخلاقی مسائل تفصیلاً بیان کریں۔

جواب: **ڈیٹا سکیورٹی سے متعلق اخلاقی مسائل (Ethical Issues Related to Security)**

ڈیٹا سکیورٹی سے متعلق اخلاقی مسائل درج ذیل ہیں:

-1 رازداری اور پوشیدگی (Confidentionality and Privacy)

دوسروں کا ڈیٹا محفوظ رکھنا درحقیقت دوسروں کی حفاظت کرنا ہے۔ مثال کے طور پر اگر بینک میرے کاروباری حریف کو میری بینکنگ ٹرانزیکشن (Banking Transaction) کی معلومات میں شریک کرتا ہے تو یہ میرے کاروبار کو نقصان پہنچا سکتا ہے۔ بالکل اسی طرح فون کمپنیوں کو invoices اور بل خفیہ طور پر رکھنے چاہییں۔ کمپیوٹر اور انٹرنیٹ کے اس دور میں رازداری اور پوشیدگی کو برقرار رکھنا مشکل ہو گیا ہے۔

کمپیوٹرز کے زیادہ استعمال کی وجہ سے ڈیٹا کی وسیع اقسام جمع اور ذخیرہ کی جاتی ہیں۔ یہ ڈیٹا کریڈٹ کارڈ، تنظیمی فنڈ کی بڑھتی ہوئی مہمات، رائے دہی ڈرائیونگ لائسنس، گرفتاری ریکارڈ اور طبی ریکارڈ سے متعلق ہو سکتی ہے۔ رازداری سے ممکنہ خطرات میں کمپیوٹر سے لیے گئے ڈیٹا کا غلط استعمال شامل ہے۔ اگر کوئی کمپنی مارکیٹنگ کے مقصد کے لیے دوسری کمپنی کو ای میل کی شناخت اور فون نمبر فروخت کرتی ہے تو یہ ڈیٹا کی رازداری کو نقصان پہنچانے کا سبب بنتی ہے۔

-2 دھوکہ دہی اور غلط استعمال

کمپیوٹر پر انٹرنیٹ استعمال کرتے ہوئے کچھ غیر قانونی سرگرمیاں فروغ پا سکتی ہیں۔ ان میں الیکٹرانک ذرائع کی مدد سے رقوم، خدمات اور قیمتی ڈیٹا کی چوری شامل ہے۔ بعض دفعہ پاس ورڈ تبدیل کرنے کے لیے ایک ای میل کے ذریعے ایک لنک پر کلک کرنے کو کہا جاتا ہے۔ جب ہم

tdleemcity.com

اس لنک پر کلک کرتے ہیں تو ایک ویب پیج کھل جاتا ہے جو ہمیں نام اور پاس ورڈ دینے کے بارے میں پوچھتا ہے۔ اگر ہم اپنا نام اور پاس ورڈ ظاہر کرتے ہیں تو کچھ نقصان پہنچانے والے صارفین ہمارا پاس ورڈ چوری کر لیتے ہیں۔ اسی طرح کچھ ای میلز ہمیں بے وقوف بنانے کی کوشش کرتی ہیں کہ آپ نے بہت قیمتی انعام جیت لیا ہے۔ مثال کے طور پر ایک گاڑی یا گھر اور وہ ہمیں اس انعام کو حاصل کرنے کے لیے منتقلی فیس کے طور پر ایک چھوٹی سی رقم ادا کرنے کا کہا جاتا ہے۔ درحقیقت یہ لوگوں کو بے وقوف بنانے اور ان سے رقم بٹورنے کا ایک ذریعہ ہے۔

بعض اوقات نقصان پہنچانے والے صارف ہمیں اپنا دوست ظاہر کر کے ہماری کچھ خفیہ معلومات حاصل کرنے کی کوشش کرتے ہیں۔ اسے Phishing کہتے ہیں۔

-3 پیٹنٹ (Patent)

پیٹنٹ کسی آئیڈیا کی حفاظت کا ایک طریقہ ہے۔ اگر آپ کسی فیلڈ میں تحقیق کر رہے ہیں اور آپ کے پاس کوئی آئیڈیا ہے تو آپ کو چاہیے کہ آئیڈیا کا پیٹنٹ حاصل کر لیں۔ یہ دوسروں کو اس آئیڈیا کی بنیاد پر کچھ ایجاد کرنے اور فروخت کرنے سے روکنے کا آپ کو حق دیتا ہے۔

-4 کاپی رائٹ قانون (Copyright Law)

کاپی رائٹ پیٹنٹ سے مختلف ہے۔ کاپی رائٹ کے قانون کے مطابق کسی بھی آئیڈیا یا چیز کو کاپی نہیں کیا جا سکتا۔ حقوق کاپی کرنے کے لیے مخصوص ہیں۔ اگر کوئی چیز کاپی رائٹ کے تحت محفوظ ہے تو ہم اس میں ایک کاپی رائٹ کا نشان رکھتے ہیں۔

-5 تجارتی راز (Trade Secrets)

تجارتی راز سے مُراد وہ راز جو کسی کمپنی کی کامیابی کے لیے نمایاں کردار ادا کریں۔ یہ کسی کمپنی کے لیے قابلِ قدر اور افادیت کے حامل ہوتے ہیں۔ کمپیوٹر سائنس کے شعبہ میں تجارتی راز پوشیدہ رکھنا نہایت اہم ہے۔ اس صورت میں جب ایک سے زائد سوفٹ ویئر کمپنیاں ایک ہی قسم کی مصنوعات تیار کرتی ہوں اور ان میں کسی ایک کو دوسری کمپنیوں پر برتری حاصل ہو سکتی ہو۔ جیسے بہت سی کمپنیاں ای میل کی خدمات فراہم کرتی ہیں لیکن ان میں سے کچھ کو دوسروں پہ نمایاں برتری حاصل ہے۔

-6 تخریب کاری (Sabotage)

تخریب کاری کمپیوٹر سسٹم پر ایک سنگین حملہ ہے۔ کچھ نقصان پہنچانے والے صارف دُور بیٹھے ہوئے ہی اس سسٹم پر حملہ کر سکتے ہیں۔ کوئی مفت سافٹ ویئر کے ذریعے وائرس بھیج سکتا ہے۔ وائرس بُرے ارادے سے لکھا گیا کمپیوٹر پروگرام ہے۔ یہ معلومات کو تبدیل یا تباہ کر سکتا ہے یا قیمتی ڈیٹا سے چھیڑ چھاڑ کر سکتا ہے۔

سوال4: رازداری اور پوشیدگی سے کیا مراد ہے؟

جواب: **رازداری اور پوشیدگی (Confidentionality and Privacy)**

دوسروں کا ڈیٹا محفوظ رکھنا درحقیقت دوسروں کی حفاظت کرنا ہے۔ مثال کے طور پر اگر بینک میرے کاروباری حریف کو میری بینکنگ ٹرانزیکشن (Banking Transaction) کی معلومات میں شریک کرتا ہے تو یہ میرے کاروبار کو نقصان پہنچا سکتا ہے۔ بالکل اسی طرح فون کمپنیوں کو invoices اور بل خفیہ طور پر رکھنے چاہییں۔ کمپیوٹر اور انٹرنیٹ کے اس دور میں رازداری اور پوشیدگی کو برقرار رکھنا مشکل ہو گیا ہے۔

کمپیوٹرز کے زیادہ استعمال کی وجہ سے ڈیٹا کی وسیع اقسام جمع اور ذخیرہ کی جاتی ہیں۔ یہ ڈیٹا کریڈٹ کارڈ، تنظیمی فنڈ کی بڑھتی ہوئی مہمات، رائے

وہی ڈرائیونگ لائسنس، گرفتاری ریکارڈ اور طبی ریکارڈ سے متعلق ہو سکتی ہے۔ راز داری سے ممکنہ خطرات میں کمپیوٹر سے لیے گئے ڈیٹا کا غلط استعمال شامل ہے۔ اگر کوئی کمپنی مارکیٹنگ کے مقصد کے لیے دوسری کمپنی کو ای میل کی شناخت اور فون نمبر فروخت کرتی ہے تو یہ ڈیٹا کی راز داری کو نقصان پہنچانے کا سبب بنتی ہے۔

سوال5: پائریسی (غیر قانونی کاپی رائٹ) سے کیا مراد ہے؟

جواب: **پائریسی (Piracy) (غیر قانونی کاپی رائٹ)**

پائریسی کا مطلب غیر قانونی نقلیں تیار کرنا ہے۔ کتاب، شاعری، سوفٹ ویئر، فلم، مصوری، گھر کا نقشہ تعمیر یا کسی ایسے کام کی خلاف قانون نقل کرنا جواز روئے قانون ممنوع ہے۔

سوال6: سافٹ ویئر پائریسی کی کتنی اقسام ہیں؟

جواب: **سافٹ ویئر پائریسی کی اقسام (Types of Software Piracy)**

سافٹ ویئر پائریسی کی مندرجہ ذیل پانچ اقسام ہیں:

(i) سافٹ لفٹنگ (ii) کلائنٹ سرور اوور یوز (iii) ہارڈ ڈسک لوڈنگ
(iv) جعل سازی (v) آن لائن پائریسی

سوال7: سافٹ لفٹنگ کیا ہوتی ہے؟

جواب: **سافٹ لفٹنگ (Softlifting)**

کسی دوسرے سے ایپلیکیشن سافٹ ویئر کی کاپی لے کر انسٹال کرنا سافٹ لفٹنگ کہلاتا ہے۔

سوال8: کلائنٹ سرور اوور یوز سے کیا مراد ہے؟

جواب: **کلائنٹ سرور اوور یوز (Client-server overuse)**

حاصل کردہ لائسنس کے مقابلے سافٹ ویئر کی مزید کاپیاں انسٹال کرنا، کلائنٹ سرور اوور یوز کہلاتا ہے۔

سوال9: ہارڈ ڈسک لوڈنگ سے کیا مراد ہے؟

جواب: **ہارڈ ڈسک لوڈنگ (Hard Disk Loading)**

تجدید شدہ یا نئے کمپیوٹر، پر غیر مجاز شدہ سافٹ ویئر کی کاپیاں انسٹال اور فروخت کرنا ہارڈ ڈسک لوڈنگ کہلاتا ہے۔

سوال10: جعل سازی کسے کہتے ہیں؟

جواب: **جعل سازی (Counterfeiting)**

سافٹ ویئر کی نقلیں تیار کرنے اور فروخت کرنے کو جعل سازی کہتے ہیں۔

سوال11: آن لائن پائریسی سے کیا مراد ہے؟

جواب: **آن لائن پائریسی (Online Piracy)**

آن لائن پائریسی میں عموماً غیر قانونی سافٹ ویئرز ڈاؤن لوڈ کرنا شامل ہے۔

سوال 12: ڈیٹا اور سیکیورٹی کے حوالے سے دھوکا اور غلط استعمال کی وضاحت کریں۔

جواب: **دھوکا اور غلط استعمال (Fraud & Misuse)**

کمپیوٹر پر انٹرنیٹ استعمال کرتے ہوئے کچھ غیر قانونی سرگرمیاں فروغ پا سکتی ہیں۔ ان میں الیکٹرانک ذرائع کی مدد سے رقوم، خدمات اور قیمتی ڈیٹا کی چوری شامل ہے۔ بعض دفعہ پاس ورڈ تبدیل کرنے کے لیے ایک ای میل کے ذریعے ایک لنک پر کلک کرنے کو کہا جاتا ہے۔ جب ہم اس لنک پر کلک کرتے ہیں تو ایک ویب پیج کھل جاتا ہے جو ہمیں نام اور پاس ورڈ دینے کے بارے میں پوچھتا ہے۔ اگر ہم اپنا نام اور پاس ورڈ ظاہر کرتے ہیں تو کچھ نقصان پہنچانے والے صارفین ہمارا پاس ورڈ چوری کر لیتے ہیں۔ اسی طرح کچھ ای میلرز ہمیں بے وقوف بنانے کی کوشش کرتی ہیں کہ آپ نے بہت قیمتی انعام جیت لیا ہے۔ مثال کے طور پر ایک گاڑی یا گھر اور وہ ہمیں اس انعام کو حاصل کرنے کے لیے منتقلی فیس کے طور پر ایک چھوٹی سی رقم ادا کرنے کا کہا جاتا ہے۔ درحقیقت یہ لوگوں کو بے وقوف بنانے اور ان سے رقم بٹورنے کا ایک ذریعہ ہے۔

بعض اوقات نقصان پہنچانے والے صارف ہمیں اپنا دوست ظاہر کر کے ہماری کچھ خفیہ معلومات حاصل کرنے کی کوشش کرتے ہیں۔ اسے Phishing کہتے ہیں۔

سوال 13: پیٹنٹ سے کیا مراد ہے؟

جواب: **پیٹنٹ (Patent)**

پیٹنٹ کسی آئیڈیا کی حفاظت کا ایک طریقہ ہے۔ اگر آپ کسی فیلڈ میں تحقیق کر رہے ہیں اور آپ کے پاس کوئی آئیڈیا ہے تو آپ کو چاہیے کہ آئیڈیا کا پیٹنٹ حاصل کر لیں۔ یہ دوسروں کو اس آئیڈیا کی بنیاد پر کچھ ایجاد کرنے اور فروخت کرنے سے روکنے کا آپ کو حق دیتا ہے۔

سوال 14: کاپی رائٹ قانون کی وضاحت کریں۔

taleemcity.com

جواب: **کاپی رائٹ قانون (Copyright Law)**

کاپی رائٹ پیٹنٹ سے مختلف ہے۔ کاپی رائٹ کے قانون کے مطابق کسی بھی آئیڈیا یا چیز کو کاپی نہیں کیا جا سکتا۔ حقوق کاپی کرنے کے لیے مخصوص ہیں۔ اگر کوئی چیز کاپی رائٹ کے تحت محفوظ ہے تو ہم اس میں ایک کاپی رائٹ کا نشان رکھتے ہیں۔

سوال 15: تجارتی راز سے کیا مراد ہے؟

جواب: **تجارتی راز (Trade Secrets)**

تجارتی راز سے مُراد وہ راز جو کسی کمپنی کی کامیابی کے لیے نمایاں کردار ادا کریں۔ یہ کسی کمپنی کے لیے قابلِ قدر اور افادیت کے حامل ہوتے ہیں۔ کمپیوٹر سائنس کے شعبہ میں تجارتی راز پوشیدہ رکھنا نہایت اہم ہے۔ اس صورت میں جب ایک سے زائد سوفٹ ویئر کمپنیاں ایک ہی قسم کی مصنوعات تیار کرتی ہوں اور ان میں کسی ایک کو دوسری کمپنیوں پر برتری حاصل ہو سکتی ہو۔ جیسے بہت سی کمپنیاں ای میل کی خدمات فراہم کرتی ہیں لیکن ان میں سے کچھ کو دوسروں پہ نمایاں برتری حاصل ہے۔

سوال 16: تخریب کاری سے کیا مراد ہے؟

جواب: **تخریب کاری (Sabotage)**

تخریب کاری کمپیوٹر سسٹم پر ایک سنگین حملہ ہے۔ کچھ نقصان پہنچانے والے صارف دُور بیٹھے ہوئے ہی اس سسٹم پر حملہ کر سکتے ہیں۔ کوئی مفت

سافٹ ویئر کے ذریعے وائرس بھیج سکتا ہے۔ وائرس بُرے ارادے سے لکھا گیا کمپیوٹر پروگرام ہے۔ یہ معلومات کو تبدیل یا تباہ کر سکتا ہے یا قیمتی ڈیٹا سے چھیڑ چھاڑ کر سکتا ہے۔

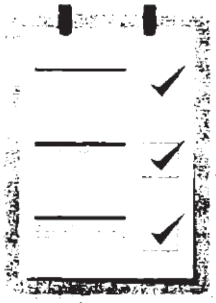
سوال17: دوسروں کی رازداری کی حفاظت کی وضاحت کریں۔

جواب: **دوسروں کی رازداری کی حفاظت (Safeguarding Privacy of Others)**

''کیمرہ آپ کو دیکھ رہا ہے'' اکثر آپ نے سڑکوں پر لگے بورڈ دیکھے ہوں گے۔ اس طرح کے نوٹس کا مقصد آپ کی رازداری کے بارے میں آپ کو متوجہ کرنا ہے تاکہ آپ قانون کی پاسداری کریں۔ اس طرح آپ کی تصویر لینے یا ویڈیو ریکارڈ کرنے سے پہلے سپیڈ کیمروں کا اعلان کیا جاتا ہے۔ یہ اقدامات صرف آپ کی رازداری کی حفاظت کرنے کے لیے ہیں۔ آپ کی معلومات نیشنل ڈیٹا بیس اینڈ رجسٹریشن اتھارٹی (NADRA) میں آپ کے دیگر خاندان کے ارکان کی معلومات کے ساتھ محفوظ کی جاتی ہیں لہٰذا اس ڈیٹا کی حفاظت نادرا کی اخلاقی اور قانونی ذمہ داری ہے۔

سوال18: ویب سائٹس کی رازداری کی پالیسیوں کی وضاحت کریں۔

جواب: **ویب سائٹس کی رازداری کی پالیسی (Privacy Policy of Website)**



زیادہ تر ویب سائٹس نے اپنی رازداری کی پالیسیوں کی نشاندہی کی ہوتی ہے جو یہ بتاتی ہیں ہے کہ وہ آپ سے متعلق اور آپ کے کمپیوٹر کی کون سی معلومات اکٹھی کرتی ہیں اور ان معلومات کا اشتراک وہ کس کے ساتھ کریں گے۔ اکثر لوگ ان پالیسیوں کو نظر انداز کرتے ہیں اور یہ سمجھتے ہیں کہ رازداری کی پالیسی کی وجہ سے ان کی رازداری مکمل طور پر محفوظ ہے۔ دراصل یہ ویب سائٹس آپ کو آگاہ کرنا چاہتی ہیں کہ وہ آپ کی رازداری کی حفاظت کس طرح کریں گے۔

سوال19: ڈیٹا کے بڑے مجموعے سے رازداری کس طرح متاثر ہوتی ہے؟

جواب: **ڈیٹا کے بڑے مجموعے سے رازداری متاثر ہونے کے خدشات**

کمپیوٹرائزڈ نظام کی وجہ سے بہت سارے ادارے آپ کے ڈیٹا کو محفوظ رکھتے ہیں۔ مثال کے طور پر

(i) ہسپتال کے پاس پیدائش، بیماری کا ریکارڈ ہو سکتا ہے۔

(ii) نادرا کے پاس آپ کے خاندان کی معلومات ہے۔

(iii) آپ کے سکول، کے پاس آپ کا ریکارڈ ہے۔

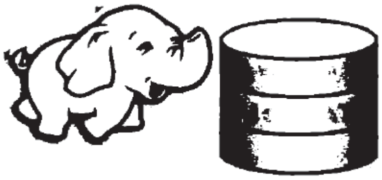
(iv) ثانوی اور اعلیٰ ثانوی تعلیمی بورڈ (BISE) کے پاس آپ کا ریکارڈ ہے۔

(v) پاسپورٹ آفس کے پاس (اگر پاسپورٹ ہے) آپ کا ریکارڈ ہے۔

(vi) ای میل سروس فراہم کرنے والوں کے پاس (اگر ای میل اکاؤنٹ ہے) کے پاس آپ کا ریکارڈ ہے۔

(vii) آن لائن سوشل نیٹ ورکنگ ویب سائٹس وغیرہ۔

لہٰذا معلومات کا ایک حصہ کسی ایک جگہ سے دوسری جگہ کسی اطلاع دیے بغیر منتقل ہو سکتا ہے۔ ایسا ڈیٹا کے بڑے مجموعہ کی وجہ سے ہے۔



سوال20: کمپیوٹنگ سسٹم کو استعمال کرنے سے پیدا ہونے والے ذاتی رازداری اور حفاظتی خدشات کا تجزیہ کریں۔

جواب: **ذاتی رازداری اور حفاظتی خدشات کا تجزیہ**

Analysis of the personal confidentiality and security concerns

ہمارے کمپیوٹرز پر انٹرنیٹ استعمال کرنے سے دوسرے کمپیوٹرز کے ساتھ منسلک ہونے کی وجہ سے بہت سے سکیورٹی خدشات بھی پیدا ہوتے ہیں۔ اس وجہ سے ہم مندرجہ ذیل پہلوؤں کے مطابق اپنے ڈیٹا کو محفوظ رکھنا چاہتے ہیں۔

(i) رازداری (Confidentiality)

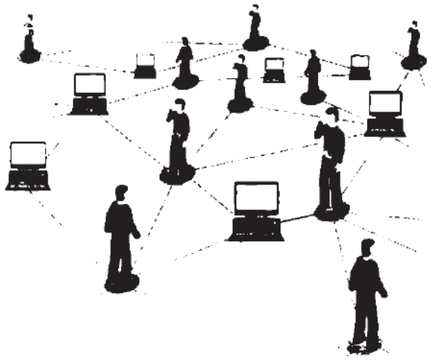
رازداری کا مطلب یہ ہے کہ ہم اپنے ڈیٹا کو خفیہ رکھنا چاہتے ہیں۔ ہم اسے غیر منظم افراد کے ساتھ اشتراک نہیں کرنا چاہتے۔

(ii) صداقت (Integrity)

ہم ڈیٹا کو درست رکھنا چاہتے ہیں۔ مثلاً بینک سے متعلقہ ریکارڈ کا درست ہونا ہم سب کی خواہش ہوتی ہے۔

(iii) دستیابی (Availability)

اس سے مراد یہ ہے کہ جب چاہیں اپنے ڈیٹا پر رسائی حاصل کر سکیں۔ کیونکہ اگر فروخت کے وقت ڈیٹا میسر نہ ہو تو پھر کچھ دوسری صورتوں میں یہ بیکار ہو جاتا ہے یہ تمام پہلو کمپیوٹرائزڈ نظام میں ڈیٹا بیس کی پروسیسنگ، اسٹوریج اور ٹرانسمیشن کے دوران بہت اہم ہیں۔ جب ہم انٹرنیٹ کو استعمال کرتے ہیں تو ہماری ذاتی معلومات پیدا ہوتی ہیں جو کسی کمپنی کی دلچسپی کا باعث بن سکتی ہیں یا دوسرے مقاصد کے لیے لوگ اسے استعمال کر سکتے ہیں وہ ان معلومات کو مارکیٹنگ کے لیے استعمال کرتی ہیں اس عمل کو رازداری پر حملہ سمجھا جاتا ہے۔



سوال21: خفیہ کاری کیا ہوتی ہے؟

جواب: **خفیہ کاری (Encryption)**

خفیہ کاری ایک ایسا عمل ہے جس کی مدد سے ڈیٹا کی ان کوڈنگ (Encoding) کی جاتی ہے۔اس طرح صرف مجاز افراد اِسے پڑھ سکتے ہیں۔

سوال22: ان کوڈنگ سے کیا مراد ہے؟

جواب: **ان کوڈنگ(Encoding)**

ان کوڈنگ کا مطلب ڈیٹا کو نہ پڑھے جاسکنے والی شکل میں تبدیل کرنا ہے جسے سائفر ٹیکسٹ (Ciphertext) کہتے ہیں۔اس ڈیٹا کو پڑھنے کے لیے ایک خفیہ کوڈ(Key) کی ضرورت ہوتی ہے۔

سوال23: روزمرہ زندگی میں انٹرنیٹ پر خفیہ کاری کی اہمیت بیان کریں۔

جواب: **روزمرہ زندگی میں انٹرنیٹ پر خفیہ کاری کی اہمیت**

(Importance of Encryption for Everyday Life on the Internet)

ڈیٹا کو سیکورٹی فراہم کرنے کے لیے خفیہ کاری کا ایک اہم طریقہ ہے۔انٹرنیٹ پر روزمرہ کی زندگی میں بہت سی ذاتی معلومات کئی مقامات پر محفوظ کی جاتی ہیں۔لہٰذا ڈیٹا کو خفیہ رکھنے کا طریقہ کار جاننا بہت ضروری ہے۔خفیہ کاری اس حوالے سے بہت اہم ہے کیونکہ یہ ڈیٹا کو غیر قانونی رسائی سے محفوظ رکھتی ہے۔خفیہ کاری کی اہمیت مندرجہ ذیل نکات میں بیان کی جاسکتی ہے:

-1 **ہیکرز سے تحفظ (Protection from Hackers)**

ہیکرز صرف معلومات چوری نہیں کرتے ہیں وہ دھوکا دینے کے لیے ڈیٹا کو تبدیل کر کے بھی فائدہ اُٹھا سکتے ہیں۔مثال کے طور پر آن لائن پیسے کی منتقلی کی بینک ٹرانزیکشن میں وہ ٹارگٹ اکاؤنٹ نمبر کو تبدیل کر کے دھوکا دے سکتے ہیں۔

-2 **خفیہ کاری رازداری کی حفاظت (Encryption Protects Privacy)**

خفیہ کاری حساس ڈیٹا سمیت افراد کی ذاتی معلومات کی بھی حفاظت کرتی ہے۔یہ رازداری کو یقینی بناتی ہے اور مجرموں کو آپ کے ڈیٹا کی نگرانی کم کرنے میں بھی مدد کرتی ہے۔

-3 **خفیہ کاری آلات میں ڈیٹا کی حفاظت کرتی ہے (Encryption Protects Data across Devices)**

ایک سے زیادہ (موبائل) آلات ہماری زندگی کا ایک بڑا حصہ ہیں اور ایک آلہ سے دوسرے آلہ کو حساس ڈیٹا منتقل کرنا ایک خطرناک عمل ہے۔خفیہ کاری تمام آلات میں ڈیٹا محفوظ کرتے وقت یہاں کے منتقل کرتے وقت ان کی حفاظت میں مدد دیتی ہے۔اضافی حفاظتی اقدامات جیسا کہ اعلیٰ درجے کی تصدیق غیر مجاز صارفین کو روکنے میں مدد کرتے ہیں۔

سوال24: سائفر ٹیکسٹ کسے کہتے ہیں؟

جواب: **سائفر ٹیکسٹ(Ciphertext)**

ڈیٹا کو نہ پڑھے جاسکنے والی شکل میں تبدیل کرنا سائفر ٹیکسٹ کہلاتا ہے۔

سوال25: ہیکر کسے کہتے ہیں؟

جواب: **ہیکر (Hacker)**

کمپیوٹر ماہر جو ڈیٹا چوری کرے اسے ہیکر کہتے ہیں۔

سوال26: متبادل سازی سے کیا مراد ہے؟ نیز متبادل سازی کے طریقے بھی بیان کریں۔

جواب: **متبادل سازی (Substitution Cipher)**

متبادل سازی خفیہ کاری کا ایک طریقہ ہے جس میں اصل متن کے حروف دوسرے حروف کے ساتھ تبدیل کر دیے جاتے ہیں۔

متبادل سازی کے طریقے (Substitution Cipher Method)

متبادل سازی خفیہ کاری کا ایک طریقہ ہے جس میں اصل متن کے حروف دوسرے حروف کے ساتھ تبدیل کر دیے جاتے ہیں۔ یہ متبادل عمل ایک مقررہ وضاحتی نظام کی مدد سے کیا جاتا ہے۔ متبادل سازی کے طریقے مندرجہ ذیل ہیں:

(i) سیزر سائیفر (ii) وگینیر سائیفر

سوال27: سیزر کون تھا؟

جواب: **سیزر (Ceaser)**

سیزر ایک رومن سیاستدان اور فوجی جنرل تھا جس نے رومن سلطنت کے عروج تک اہم کردار ادا کیا۔ سیزر نے اپنے فوجیوں اور جرنیلوں کو پیغامات بھیجنے کے لیے ایک خفیہ کاری کا طریقہ استعمال کیا۔ اس طریقے کو سیزر سائیفر کہا جاتا ہے۔

سوال28: سیزر سائیفر طریقہ کیا ہوتا ہے؟

جواب: **سیزر سائیفر طریقہ (Caeser Cipher Method)**

سیزر نے اپنے فوجیوں اور جرنیلوں کو پیغامات بھیجنے کے لیے ایک خفیہ طریقہ استعمال کیا۔ اس طریقے کو سیزر سائیفر طریقہ کہا جاتا ہے۔ اس طریقے میں ہم حروف تہجی کو تحریر کرتے وقت دوسرے حروف سے تبدیل کر دیتے ہیں۔ حروف کی ترتیب میں اصل حروف تہجی کے بائیں یا دائیں کے لیے کچھ طے شدہ نمبر ہوتے ہیں۔

taleemcity.com

مثال1: معیاری انگریزی حروف تہجی کے "تین حروف دائیں جانب متبادل" سے ہمیں مندرجہ ذیل نتائج حاصل ہوتے ہیں۔

ابتدائی حروف: ABCDEFGHIJKLMNOPQRSTUVWXYZ

خفیہ کاری حروف: DEFDEFGHIJKLMNOPQRSTUVWABC

مثال2: معیاری انگریزی حروف تہجی کے "پانچ حروف دائیں جانب متبادل" سے ہمیں مندرجہ ذیل نتائج حاصل ہوتے ہیں۔

ابتدائی حروف: ABCDEFGHIJKLMNOPQRSTUVWXYZ

خفیہ کاری حروف: FGHIJKLMNOPQRSTUVWXYZABCDE

اس متبادل طریقے کے تحت، سادی عبارت "PAKISTAN" خفیہ کاری میں "UFPNXYFS" میں تبدیل ہو جائے گی۔

سوال29: وگینیر سائیفر سے کیا مراد ہے؟

جواب: **وگینیر سائیفر (Vigenere Cipher)**

وگینیر سائیفر ایک دوسرا متبادل سائیفر ہے جس میں سادہ عبارت کے حروف کو تبدیل کرنے کے لیے ایک ٹیبل کا استعمال کیا جاتا ہے جسے وگینیر سائیفر ٹیبل کہتے ہیں۔

جواب: وگنیئر سائیفر ٹیبل(Vigenere Cipher Table)

یہ ٹیبل چھبیس قطاروں اور چھبیس کالموں پر مشتمل ہے۔ جہاں پہلی قطار میں اصل A–Z حروف تہجی ہیں۔ باقی ہر قطار میں حروف تہجی کو ایک خط بائیں طرف منتقل کر دیا جاتا ہے۔ تمام کالموں کو حروف تہجی میں A–Z تک لیبل (Label) کر دیا جاتا ہے اور اس طرح تمام قطاروں کو بھی A–Z تک لیبل کر دیا جاتا ہے۔

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	[illegible]	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	[illegible]	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	[illegible]	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	[illegible]	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	[illegible]	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	[illegible]	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	[illegible]	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	[illegible]	A	[illegible]	[illegible]	D	[illegible]	[illegible]	G	[illegible]	[illegible]	[illegible]	[illegible]	L	[illegible]	[illegible]	O	P	Q	R	S	T	U	V	W	X	Y

taleemcity.com

سوال 31: وگنیئر سائیفر طریقہ بیان کریں۔

جواب: **وگنیئر سائیفر طریقہ(Vigenere Cipher Method)**

اس طریقے سے ہمارے پاس ایک متبادل کلید(Key) ہوتی ہے جسے سادہ عبارت کے ساتھ ملا دیا جاتا ہے جس سے سائیفر ٹیکسٹ(Cipher Text) بنتا ہے۔ ہم سادہ عبارت کے ہر حرف کو خفیہ کاری میں تبدیل کرنے کے لیے وگنیئر ٹیبل کے کالم میں تلاش کرتے ہیں وگنیئر سائیفر ٹیبل اور اس کالم میں ہم اُس حرف کو تلاش کرتے ہیں جو کلید(Key) کے متعلقہ حرف کے سامنے ٹیبل کی قطار میں آ رہا ہے۔ ہم یہ عمل جاری رکھتے ہیں جب تک کہ ساری عبارت ختم نہ ہو جائے۔

مثال: فرض کریں ہم کلید "ZINDABAD" کی مدد سے عبارت "PAKISTAN" کی خفیہ کاری میں کرنا چاہتے ہیں۔ ہم خط 'P' کو پہلا خط سادہ عبارت میں) کالم لیبلز میں اور خط 'Z' کو (متبادل کلید کا پہلا خط) قطار لیبلز میں تلاش کرتے ہیں۔ ہم دیکھ سکتے ہیں کہ قطار اور کالم خط 'O' پہ ملتے ہیں جو کہ پیلے رنگ سے لکھا ہوا ہے۔ دیکھیں وگنیئر سائیفر ٹیبل۔ لہٰذا خط 'P' خط 'O' سے تبدیل ہو جائے گا۔ اس طرح ہم خط 'A' کو کالم لیبلز میں اور خط 'I' کو قطار لیبلز میں تلاش کریں گے جیسا کہ وگنیئر سائیفر ٹیبل میں ملاحظہ کیا جا سکتا ہے۔ قطار اور کالم خط 'I' پر ملتے ہیں اس لیے خط 'A' خط 'I' میں تبدیل ہو جائے گا۔ اس طرح لفظ "PAKISTAN" خفیہ کاری کے حوالے سے لفظ "QIXLSUAQ" میں تبدیل ہو جائے گا جیسا کہ ٹیبل میں دکھایا گیا ہے۔

Column Label	P	A	K	I	S	T	A	N
Row Label	Z	I	N	D	A	B	A	D
Common Letter	O	I	X	L	S	U	A	Q

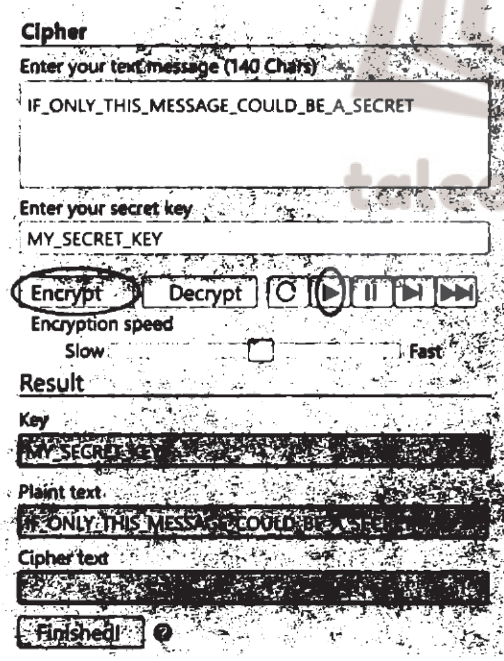
اہم نوٹ: اگر کلید کے حروف کی تعداد عبارت کے حروف سے کم ہو تو ہم کلید کے حروف کو شروع سے دوبارہ لکھیں گے۔ مثال کے طور پر لفظ "PAKISTAN" جس کے آٹھ حروف میں کو کلید (Key) "BEAUTY" جس کے چھ خطوط میں سے خفیہ کاری میں تبدیل کرنا چاہتے ہیں تو ہم کلیدی حروف کو دیے گئے لفظ میں لمبائی میں برابر کرنے کے لیے دوبارہ لکھیں گے۔ لہٰذا کلید "BEAUTY BE" بن جائے گی جس کے حروف دی گئی عبارت سے برابر ہیں۔ اس طریقے کو ہم اِنیٹرم سائیفر ٹیکسٹ (Interim Ciphertext) کہتے ہیں۔

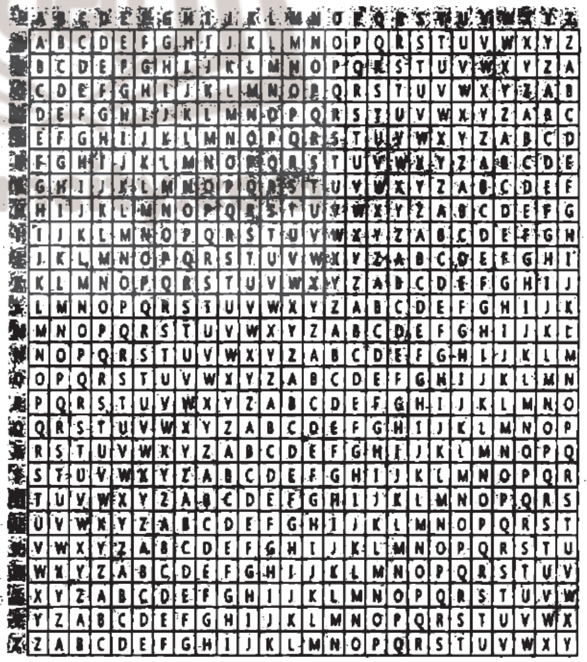
سوال 32: وگنیئر سائیفر وجیٹ کا استعمال بیان کریں۔

جواب: **وگنیئر سائیفر وجیٹ کا استعمال (Use of Vigenere Cipher Widget)**

ویب سائٹ https://studio.code.org/s/frequency_analysis/stage/1/puzzle/1 پر ایک وجیٹ دستیاب ہے اسے وگنیئر سائیفر خفیہ کاری وجیٹ کہا جاتا ہے۔ یہ دی گئی کلید کے مطابق وگنیئر سائیفر کا استعمال کرتے ہوئے سادہ عبارت کی خفیہ کاری اور decryption کو حرکت پذیری (animation) کی صورت میں دکھاتی ہے۔ اس وجیٹ کی تصاویر کو شکل 4.13 میں دکھایا گیا ہے۔

آپ اوپر دائیں کونے پر عبارت لکھ سکتے ہیں اور خفیہ کاری کے لیے ایک کلید (Key) فراہم کر سکتے ہیں۔ خفیہ کاری کے بٹن کو دبائیں اور اس کے بعد خفیہ کاری کی حرکت پذیری کے لیے کلک کریں۔ دونوں بٹنوں پر دائرے کا نشان ہے۔ جیسا شکل میں دکھایا گیا ہے۔ اسی طرح اصل پیغام دیکھنے کے لیے سائیفر عبارت کو منسوخ کر سکتے ہیں۔





	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

سوال 33: پیغام ڈیکرپٹ کرنے کا عمل بیان کریں۔

جواب: **ایک پیغام ڈیکرپٹ کرنے کا عمل (Process of Decrypt a message)**

پیغام ڈیکرپٹ کرنے کے لیے وگنیئر ٹیبل کی قطاروں میں کی لیٹرز تلاش کرتے ہیں۔ اور پھر اس قطار میں مخفی عبارت کا حرف تلاش کرتے ہیں۔

جب حرف مل جاتا ہے تو ہم اس حرف کے کالم کی سرخی کو ڈیکرپٹ حرف کے طور پر لیتے ہیں۔ مثال کے طور پر "OXLSUAQ" لفظ کو کلید لفظ "ZINDABAD" کے لحاظ سے ڈیکرپٹ کرنے کے لیے ہم خط 'Z' کی قطار تلاش کریں گے اور ان قطاروں میں ہم خط 'O' تلاش کریں گے جہاں ہم کالم کی سرخی کی شناخت کر سکتے ہیں۔ جیسا کہ اس صورت میں 'P' ہم اس عمل کو سائیفر عبارت کے ہر حرف کے لیے جاری رکھیں گے اور سائیفر عبارت کو ڈیکرپٹ کریں گے۔

سوال34: بے ترتیب متبادل خفیہ کاری سے کیا مراد ہے؟

جواب: **بے ترتیب متبادل خفیہ کاری (Random Substitution Cipher)**

سیزر سائیفر کے استعمال سے بنائے گئے پیغامات کو توڑنا بہت آسان ہے۔ اگر پورے لفظ کو ایک ہی ترتیب سے خفیہ پیغام میں تبدیل کرنے کے بجائے لفظ کے ہر خط کو بے ترتیب مختلف لیٹرز (الفاظ) سے تبدیل کرتے ہیں۔ یہ بے ترتیب متبادل سیزر سائیفر کہلاتا ہے۔

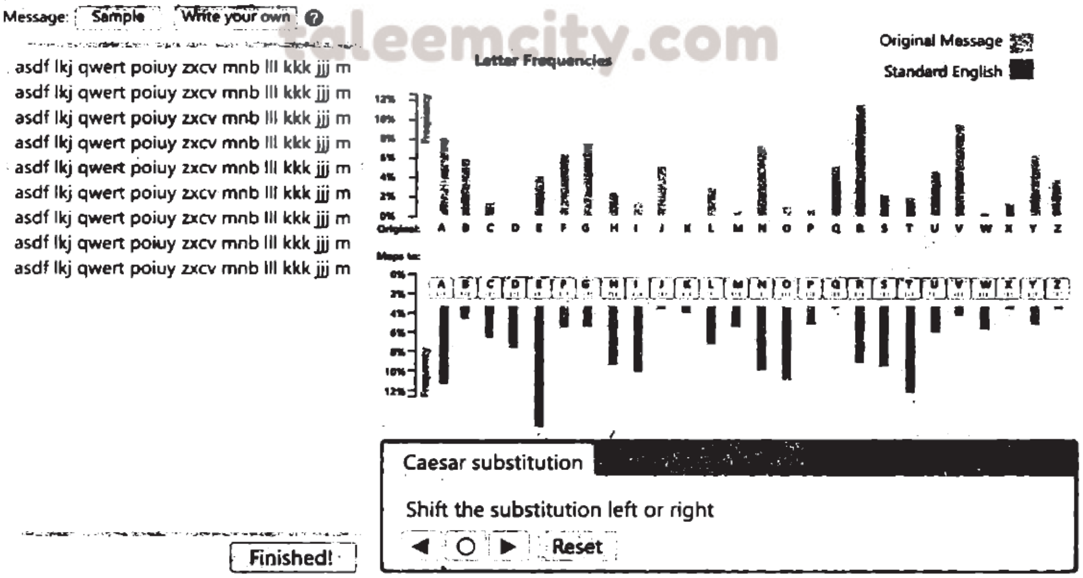
سوال35: فریکوئینسی تجزیہ استعمال کرتے ہوئے بے ترتیب متبادل کے ساتھ خفیہ کاری کے بارے میں بیان کریں۔

جواب: **فریکوئینسی تجزیہ استعمال کرتے ہوئے بے ترتیب متبادل کے ساتھ خفیہ کاری**

(Encrypted with Random Substitution using Frequency Analysis)

سیزر سائیفر (Caesar Cipher) کے استعمال سے بنائے گئے پیغامات کو توڑنا بہت آسان ہے۔ اگر پورے لفظ کو ایک ہی ترتیب سے خفیہ پیغام میں تبدیل کرنے کے بجائے لفظ کے ہر خط کو بے ترتیب مختلف لیٹرز سے تبدیل کرتے ہیں۔ یہ بے ترتیب متبادل سیزر سائیفر (Caesar Cipher) کہلاتا ہے۔

ہم ویب سائٹ کا ملاحظہ کر سکتے ہیں۔ https://studio.code.org/s/frequency_analysis/stage/1/puzzle/1 اس مقصد کے لیے ویجیٹ کو دیکھ سکتے ہیں۔ اس کی تصاویر شکل میں دیکھی جا سکتی ہیں۔



آپ کے خفیہ کردہ پیغام میں سب سے زیادہ استعمال ہونے والا 'E' کے ساتھ تبدیل ہو سکتا ہے۔ Cryptanalysis سائیفر پیغام میں حروف یا گروپوں کی فریکوئینسی کا مطالعہ ہے۔ یہ طریقہ کار کلاسیکل سائیفر کو توڑنے کے لیے امداد کے طور پر استعمال کیا جاتا ہے۔

سوال 36: متبادل سائیفر کے نقائص بیان کریں۔

جواب: متبادل سائیفر کے نقائص (Replacement cipher defects)

تمام متبادل سائیفر میں یہ سب سے آسان ہے کیونکہ سائیفر حروف تہجی محض حروف تہجی کی ایک دائروی تبدیلی ہے۔ اس کمزوری کی وضاحت یہ ہے کہ سادہ عبارت اور سائیفر عبارت علامتوں کی فریکوینسی کی تقسیم ایک جیسی ہے صرف علامات کو ریلیبل (Relabel) کر دیا جاتا ہے۔ سادہ متبادل سائیفر کے ساتھ ایک اور اہم مسئلہ یہ ہے کہ حروف کی تعداد بالکل ماسکڈ (Masked) نہیں ہوتی۔

سوال 37: کرپٹوگرافک کیز اور پاس ورڈز کے درمیان تعلقات کی وضاحت کریں۔

جواب: کرپٹوگرافک کیز اور پاس ورڈز کے درمیان تعلقات

(Relationship between Cryptographic Keys and Password)

پاس ورڈز کو ایک سسٹم تک رسائی حاصل کرنے کے لیے تصدیق کے طور پر استعمال کیا جاتا ہے جبکہ خفیہ کاری پیغام کو پڑھنے کے لیے کرپٹوگرافک کیز کا استعمال کیا جاتا ہے۔ لہٰذا کمپیوٹر سیکورٹی کے حوالے سے کی (Key) اور پاس ورڈ (Password) ہم معنی نہیں ہیں۔ یہ بھی ممکن ہے کہ پاس ورڈ کو کی (Key) کے طور پر استعمال کیا جا سکتا ہے۔ ان دونوں میں بنیادی فرق یہ ہے کہ پاس ورڈ کو بنانا، پڑھنا اور یاد رکھنا انسانی عمل ہے۔ کچھ سرور کمپیوٹرز پاس ورڈ آپ کے کمپیوٹر پر ہی محفوظ کرتے ہیں۔ اگلی دفعہ استعمال پر یہ ہی پاس ورڈ استعمال کیا جاتا ہے۔ جبکہ کی (Key) ایک پیغام کو پراسس (Process) کرنے کے لیے کسی کرپٹوگرافک الگورتھم (Cryptographic algorithm) کے ذریعے کوئی سافٹ ویئر یا انسان استعمال کر سکتا ہے۔

سوال 38: اچھے پاس ورڈ کی خصوصیات بیان کریں۔

جواب: اچھے پاس ورڈ کی خصوصیات (Characteristics of a Good Password)

اچھے پاس ورڈ کا اندازہ لگانا اور اس میں دراڑ پیدا کرنا مشکل ہونا چاہیے۔ یہ غیر مجاز افراد کو فائلوں، پروگراموں اور دیگر وسائل تک رسائی سے روکتا ہے۔ ایک اچھے پاس ورڈ کی مندرجہ ذیل خصوصیات ہو سکتی ہیں:

- یہ کم سے کم آٹھ حروف پر مشتمل ہو۔
- یہ آپ کے یوزر نیم (Username)، عرف، بچے کا نام یا کمپنی کے نام پر مشتمل نہ ہو۔
- یہ مکمل لفظ پر مشتمل نہ ہو۔
- یہ گزشتہ پاس ورڈز سے نمایاں طور پر مختلف ہو۔
- یہ بڑے حروف، چھوٹے حروف، نمبر اور علامات پر مشتمل ہو۔

سوال 39: سائبر کرائم کسے کہتے ہیں؟ اور سائبر کرائم کی اقسام تفصیلاً بیان کریں۔

جواب: سائبر کرائم (Cybercrime)

ایک جرم جس میں کمپیوٹر نیٹ ورک یا آلات استعمال کیے جاتے ہیں، اسے سائبر کرائم کہتے ہیں۔ مثلاً شناخت کی چوری، ٹرانزیکشن فراڈ، ایڈوانس فیس فراڈ ہیکنگ اور پائریسی وغیرہ۔

سائبر کرائم کی اقسام (Types of Cybercrime)

سائبر کرائم کی مندرجہ ذیل اقسام ہیں:

(i) شناخت کی چوری (Identity Theft)

سائبر کرائم کی ایک عام شکل شناخت کی چوری (Identify theft) ہے۔ ہیکرز پاس ورڈ اور اکاؤنٹ کی معلومات حاصل کرنے کے لیے جعلی ای میلز کا استعمال کر سکتے ہیں۔

(ii) ٹرانزیکشن فراڈ (Transaction Fraud)

مالی دھوکا دہی آن لائن میدان میں ایک عام جرم ہے۔ ایک سکیمر (Scammer) ویب سائٹ کے ذریعے فروخت کے لیے کسی چیز کی پیشکش کر سکتا ہے جب کہ وہ ادائیگی وصول کرنے کے بعد آپ کو مطلوبہ چیز نہ دینے کا ارادہ کرتے ہوئے کوئی چیز خرید سکتا ہے۔ یہ بھی ممکن ہے کہ آپ اپنے کریڈٹ کارڈ سے کچھ چیزیں خریدیں اور پھر کارڈ چوری کی اطلاع کر دیں۔ اگر کارڈ ہولڈر چارج بیک (Charge back) کا دعویٰ کرتا ہے تو اسے ٹرانزیکشنل فراڈ (Transactional fraud) کہتے ہیں۔

(iii) ایڈوانس فیس فراڈ (Advance Fee Fraud)

کبھی کبھی ہیکرز ایک بڑا انعام جیتنے پر آپ کو مبارک باد دیتے ہیں اور پھر آپ کو ایک چھوٹی سی رقم ادا کرنے کے لیے کہتے ہیں تا کہ آپ کو انعام بھیجا جا سکے۔ یہ سائبر کرائم کی ایک عام قسم ہے۔ آسانی سے دولت کمانے کے لالچ کی وجہ سے بہت سارے لوگ اس فراڈ کا شکار ہو جاتے ہیں۔

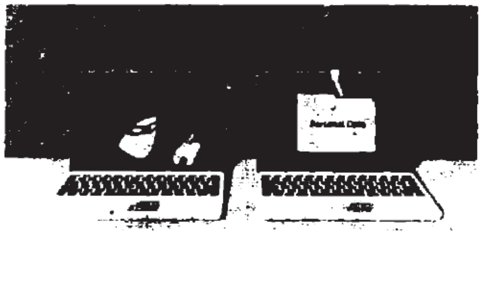
(iv) ہیکنگ (Hacking)

ہیکنگ سائبر کرائم کی ایک اور شکل ہے۔ غیر قانونی طور پر کسی دوسرے کے کمپیوٹر تک رسائی حاصل کرنا ہیکنگ کہلاتا ہے۔ یہ زیادہ تر اُس وقت ہوتا ہے جب آپ انٹرنیٹ سے کوئی فائل ڈاؤن لوڈ کرتے ہیں اور بغیر تفصیلات جانے اسے استعمال کرتے ہیں۔ آپ کا انسٹال کردہ سافٹ ویئر آپ کی اجازت کے بغیر آپ کے کمپیوٹر کو کسی دوسرے کے ساتھ جوڑ دیتا ہے۔ اس کا مقصد کسی شخص یا تنظیم کے علم میں لائے بغیر اس کی معلومات جمع کرنا ہے۔ اس قسم کے سافٹ ویئر کو سپائی ویئر (Spyware) کہتے ہیں جیسا کہ شکل میں دکھایا گیا ہے۔

سوال 40: فشنگ کسے کہتے ہیں؟ نیز فشنگ ای میل کی خصوصیات بھی بیان کریں۔

جواب: **فشنگ (Phishing)**

پاس ورڈ اور کریڈیٹ کارڈ جیسی حساس معلومات ای میل کے ذریعے حاصل کرنے کی ایک جعل ساز کوشش کو فشنگ کہتے ہیں۔



فشنگ ای میل کی خصوصیات (Characteristics of Phishing Email)

-1 یہ عام طور پر اہم نوٹس، فوری طور پر اپ ڈیٹ یا انتباہ کے طور پر ظاہر ہوتا ہے۔ ایسی ای میل کا موضوع اس طرح لکھا جاتا ہے کہ ای میل وصول کنندہ کا خیال ہوتا ہے کہ ای میل ایک قابل اعتماد ذریعے سے آئی۔

for notes, past papers, free test sessions and guess papers visit taleemcity.com

مثال (Example)

-i کسی نے آپ کا اکاؤنٹ کھولا اور فوری طور پر اس کا پاس ورڈ تبدیل کر دیا

-ii سرکاری ڈیٹا کی بریچ نوٹیفکیشن(Breach Notification)

-iii اپنے گھر کے پتے پر پیکٹ کی ترسیل

-iv آئی ٹی یاددہانی: آپ کا پاس ورڈ چوبیس گھنٹوں میں بیکار ہو جائے گا۔

-v پاس ورڈ کی تبدیلی فوری طور پر ضروری ہے

-vi نظر ثانی شدہ چھٹی اور بیمار وقت کی پالیسی

-vii ای میل اکاؤنٹ اپ ڈیٹس

-2 کبھی کبھار یہ پیغامات دھمکی دینے کے بجائے پُرکشش آواز میں ہوتے ہیں مثلاً وصول کنندہ کو تحفہ یا انعام کی یقین دہانی کرواتے ہیں۔

-3 یہ عام طور پر بھیجنے والے کا جعلی ایڈریس استعمال کرتے ہیں۔ مثال کے طور پر admin@facebook.com وغیرہ۔ اگر یہ ای میل info@gmail.com سے ہے تو آپ بھی اس ای میل کو کھول سکتے ہیں۔ ہوسکتا ہے کہ اس ای میل میں کچھ لنک ہوں جن کا آپ کے سکول کے ساتھ کوئی تعلق نہیں ہوتا۔ لہٰذا آن لائن فارم بھرنے کے دوران، ویب براؤزر کے ایڈریس بار (URL) کا خیال رکھیں۔

-4 یہ عام طور پر مواد جیسے علامات، اصلی ویب سائٹ سے تصاویر کو دھوکا دینے والی ای میل اس طرح لگاتے ہیں کہ وہ حقیقی ای میل لگے۔

-5 یہ ذاتی معلومات کو بھرنے کی خاطر وصول کنندہ کے لیے ایک فارم پر مشتمل ہوسکتا ہے۔ اور وصول کنندہ اسے فارم پر لکھ سکتا ہے۔ یہ معلومات مختلف ڈیٹا بیس میں سٹور کی جا سکتی ہیں۔

سوال 41: فشنگ ویب سائٹ کی خوبیاں بیان کریں۔

جواب: **فشنگ ویب سائٹ کی خوبیاں (Characteristics of Phishing Website)**

فشنگ ویب سائٹ کی خوبیاں مندرجہ ذیل ہے:

-1 یہ کچھ مواد جیسے تصاویر، متن، علامات، رنگ سکیم وغیرہ کی وجہ سے اصل دکھائی دیتی ہے۔

-2 یہ اصل ویب سائٹ کے لنک پر مشتمل ہوسکتی ہے۔ جیسا کہ ہم سے رابطہ کریں، رازداری یا دستبرداری کا اعلان جس سے دیکھنے والے کو دھوکا ہو سکتا ہے۔

-3 یہ اصل ویب سائٹ پر استعمال ہونے والے نام استعمال کر سکتی ہے۔

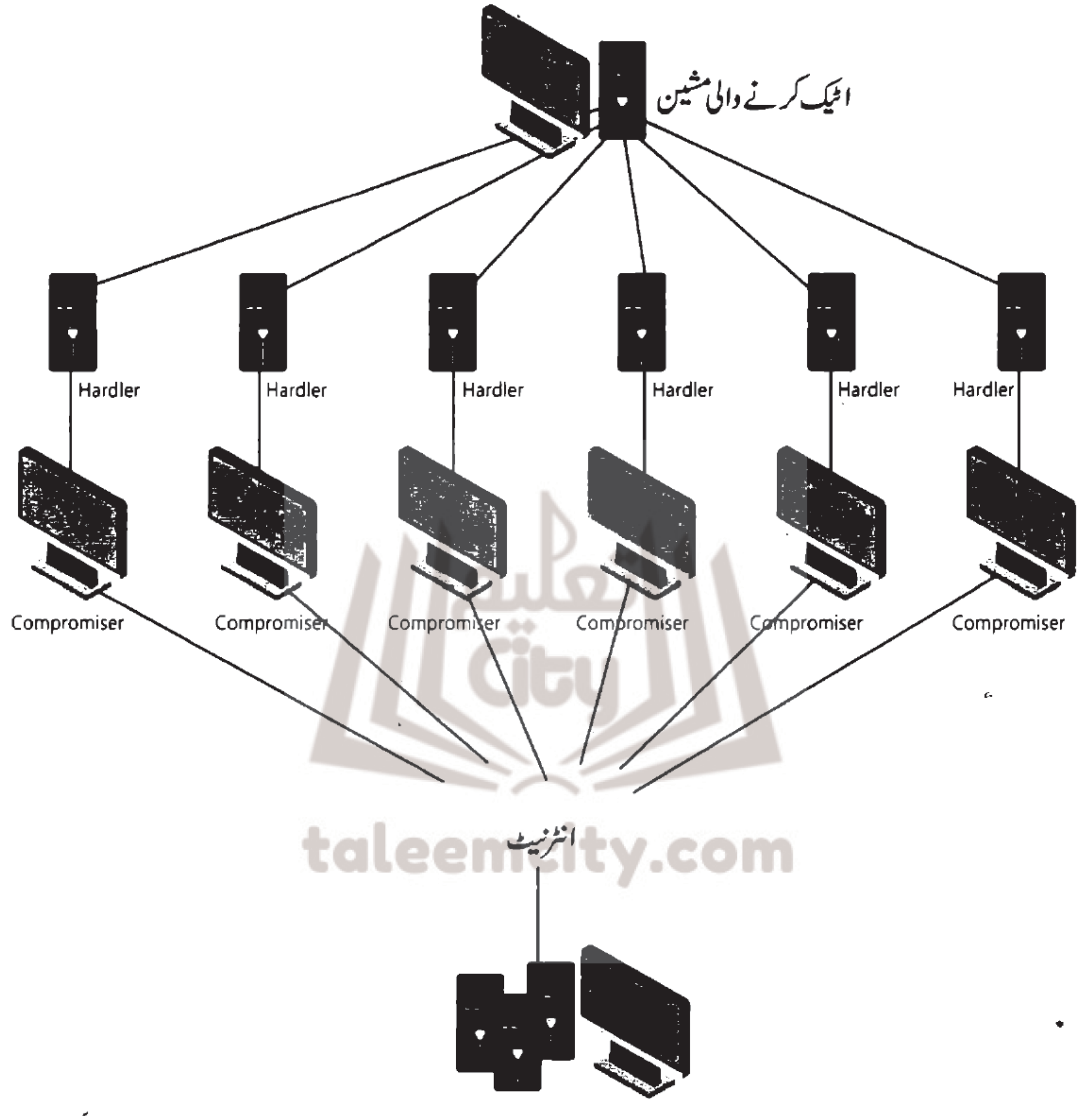
-4 یہ دیکھنے والوں کی معلومات جمع کرنے کے لیے ایسے فارم استعمال کر سکتے ہیں جو کہ اصل ویب سائٹ پر موجود فارم کی طرح ہوتے ہیں۔

سوال 42: DOS (Dedial of Service) اٹیک سے کیا مراد ہے؟

جواب: **DOS (Dedial of Service) اٹیک**

کمپیوٹنگ میں ایک مشین یا نیٹ ورک کو بیکار بنانے کے لیے DOS اٹیک کیا جاتا ہے جو کہ سائبر اٹیک کی ایک قسم ہے۔ اس کا مطلب ہے کہ آپ کی سروس کام کرنا چھوڑ گئی ہے۔ مثال کے طور پر اگر آپ کسی ویب سائٹ کو کھولنا چاہتے ہیں لیکن کوئی دوسرا شخص کمپیوٹر پروگرام کا استعمال کرتے ہوئے اسی ویب سائٹ پر بہت سی درخواستیں (Requests) پہلے ہی بھیج رہا ہے تو اس وجہ سے آپ اس ویب سائٹ تک رسائی

حاصل نہیں کر سکیں گے۔ یہ اس طرح ہے کہ کوئی روبوٹ (Robot) تھوڑے سے وقت میں بہت ساری درخواستیں بھیج رہا ہو جس کے نتیجے میں یہ سروس دوسرے صارفین کے لیے بہت سست کام کرتی ہے یا پھر کام کرنا بند کر دیتی ہے۔ لہٰذا یہ ہدف شدہ مشین یا وسائل کو زبردست درخواستوں کی مدد سے سسٹم کو اوورلوڈ (Overload) کرنے کی ایک کوشش ہے۔ یہ ایک مشین یا نیٹ ورک کو بند کرنے کا باعث بھی بن سکتا ہے۔



DOS حملہ آور عموماً اعلیٰ پروفائل تنظیموں جیسے: بینک، تجارت، میڈیا کمپنیوں یا حکومت اور تجارتی تنظیموں کے ویب سرورز کو ہدف بناتے ہیں۔ اگرچہ DOS حملوں کو عام طور پر اہم معلومات یا دیگر اثاثے چوری نہیں ہوتے تاہم یہ متاثرین کا وقت اور پیسہ خرچ کرواسکتے ہیں۔

سوال 43: DOS حملہ آور کے حدف بیان کریں۔

جواب: **DOS حملہ آور کے حدف**

DOS حملہ آور عموماً اعلیٰ پروفائل تنظیموں جیسے بنک، تجارت، میڈیا کمپنیوں یا حکومت اور تجارتی تنظیموں کے ویب سرورز کو ہدف بناتے ہیں۔ اگرچہ DOS حملوں کو عام طور پر اہم معلومات یا دیگر اثاثے چوری نہیں ہوتے۔ تاہم یہ متاثرین کا وقت اور پیسہ خرچ کرواسکتے ہیں۔

سرگرمی 4.1

آپ ٹیکسٹ کو خفیہ رکھنے کے لیے ایک طریقہ اختیار کر سکتے ہیں جیسے کہ آپ ہر لفظ کے حروف اُلٹی ترتیب سے لکھ سکتے ہیں۔
جیسے: "I like my school" کو "I ekil ym loohcs" میں تبدیل کیا جا سکتا ہے۔ ایک دوسرا طریقہ یہ ہے کہ ہر طرح حرف کی جگہ پر اگلا حرف ڈال دیا جائے مثلاً 'a' 'b' بن جائے گا اور 'b' بن جائے گا 'c' اور 'z' بن جائے گا 'a'۔ اس طرح "I like my school" بن جائے گا "J milf nz tdippm"۔
اپنا خود کا طریقہ استعمال کرتے ہوئے پاکستان کے شہروں کے نام اینکرپٹ کریں اور ان ناموں کی شناخت کے لیے اپنے دوستوں کو کی (Key) دیں۔

حل:

ابتدائی حروفِ تہجی	ABCDEFGH1JKLMNOPQRSTUVWXYZ
خفیہ کاری حروفِ تہجی	BCDEFGHIJKLMNOPQRSTUVWXYZA
LAHORE کا خفیہ کوڈ	LAHORE = MBIPSF
KASUR خفیہ کوڈ	KASUR = LBTVS

سرگرمی 4.2

اگر آپ اپنی تحریر کو آئینے کے سامنے کریں تو تحریر الٹ دکھائی دیتی ہے۔ آپ آسانی سے آئینے میں نظر آنے والی تحریر کی طرح کوئی نوٹ یا اس طرح کا کچھ اور لکھ سکتے ہیں۔ سفید یا ہلکے رنگ کی کاغذ کی ایک باریک شیٹ لیں اور اس کے ایک طرف سیاہ قلم سے کچھ لکھیں اس بات کو یقینی بنائیں کہ آپ نے کافی موٹے اور سیاہ قلم سے لکھا ہے تاکہ وہ دوسری جانب دکھائی دے۔ کاغذ کو عقبی جانب الٹائیں اور جہاں آپ نے لکھا ہے اس کا پتہ لگائیں۔ اس کے بعد عقبی جانب خاکہ بنائیں۔ یہ ایسا ہونا چاہیے جیسا کہ آپ اپنی عام تحریر کو آئینے میں دیکھتے ہیں۔ اسی طرح آپ مختلف الفاظ لکھیں، یا کسی کو ایک نوٹ لکھیں پھر اسے الٹا کریں اور انھیں بھیج دیں۔

حل: خود حل کریں۔

سرگرمی 4.3

تین متبادل حروف کو سادہ عبارت "PAKISTAN" کے بائیں طرف استعمال کرتے ہوئے خفیہ کاری میں تبدیل کریں۔

حل:

ابتدائی حروفِ تہجی	ABCDEFGH1JKLMNOPQRSTUVWXYZ
خفیہ کاری کے حروف تہجی	DEFGHIJKLMNOPQRSTUVWXYZABC
PAKISTAN کا خفیہ کوڈ	SDNLWWDQ

سرگرمی 4.4

اس کھیل کے لیے ایک چارٹ تیار کریں جو آپ، سب سے زیادہ پسند کرتے ہیں۔اس چارٹ میں اپنے پسندیدہ کھلاڑیوں کے نام سادہ الفاظ میں اور سائیفر ٹیکسٹ (Cipher Text) میں لکھیں۔آپ اپنی پسند کی کلید (Key) استعمال کر سکتے ہیں۔

حل: خود حل کریں

سرگرمی 4.5

پیغام ڈراپ ڈاؤن سے نمونہ پیغام ڈاؤن لوڈ کریں یہ ایک ایسے پیغام کو لوڈ کرے گا جو بے ترتیب متبادل سائیفر کے ساتھ خفیہ کیا گیا ہے۔آپ اندازے سے اصل سائیفر عبارت میں موجود حروف تہجی کے ہر لیٹر کو تبدیل کرتے ہوئے پیغام کو توڑ دیں گے۔آپ اصل سائیفر عبارت میں جس خط کو تبدیل کرنا چاہتے ہیں تو اسے آپ حروف تہجی کے نیلے خطوط کو براہ راست کھینچ کر نارنجی حروف کے نیچے لا سکتے ہیں۔خطوط کو آپ کے اندازے کے مطابق تبدیل کیے گئے ہیں۔اب بائیں طرف پیغام کی ونڈو (Window) میں ان کو نارنجی رنگ میں نمایاں نہیں جائے گا۔بے ترتیب متبادل سائیفر ٹیب میں دستیاب کچھ ترتیب دہ اختیارات (Sorting option) کے ساتھ کھیلیں۔Input text کے ساتھ ساتھ معیاری انگریزی عبارت میں حروف کی تعداد پر مختلف خیالات حاصل کرنے کے لیے اس کا استعمال کریں۔اس آلے کے اس وزن میں آپ گراف ساتھ مزید بات چیت کریں گے جو خط کی تعداد دکھائے گا۔

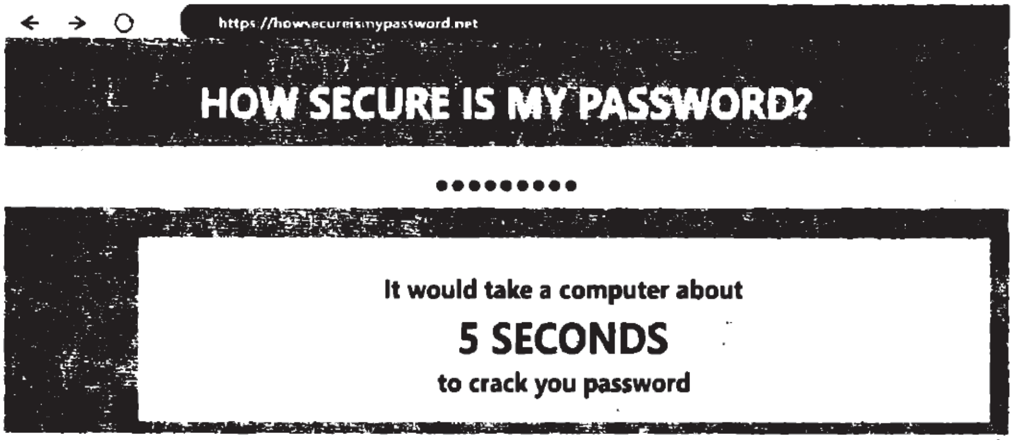
حل: خود حل کریں

سرگرمی 4.6

تمام طلبہ کمپیوٹر لیبارٹری میں جائیں اور مندرجہ ذیل ویب سائٹ تک رسائی حاصل کریں:

http://howsecureismypassword.net

وقت نوٹ کریں کہ کتنی دیر میں کمپیوٹر آپ کے پاس ورڈ کو تلاش کر سکتا ہے۔اس سکرین شارٹ کو شکل میں دکھایا گیا ہے۔کلاس ٹیچر اس قسم کی یوٹیلیٹی کی نشاندہی کرنے میں مدد کر سکتا ہے۔



حل: خود حل کریں

سرگرمی 4.7

سائبر کرائم کی اقسام httpL//nrse.gov.pk پر تلاش کریں اور ہر ایک کے بارے میں نوٹ لکھیں۔ اساتذہ طالب علموں کے گروپ بنا سکتے ہیں اور ہر گروپ کو ہر قسم پر چارٹ بنانے کے لیے کہہ سکتے ہیں۔

حل: خود حل کریں

خلاصہ Summary

-1 انٹرنیٹ پر ڈیٹا بھیجتے ہوئے ہمیں کیا خیال کرنا چاہیے؟

جواب: ہمیں انٹرنیٹ پر ڈیٹا بھیجتے ہوئے محتاط رہنے کی ضرورت ہوتی ہے۔

-2 ڈیٹا کی رازداری اور تحفظ کی ذمہ کس کی ہوتی ہے؟

جواب: ہر وہ تنظیم جس کو ڈیٹا منتقل کیا جاتا ہے ڈیٹا کی رازداری اور تحفظ اُس کی ذمہ داری ہے۔

-3 پائریسی کا کیا مطلب ہے؟

جواب: پائریسی (Piracy) کا مطلب ہے مالک کی اجازت کے بغیر سافٹ ویئر کی غیر قانونی اور غیر مجاز شدہ نقل۔

-4 سافٹ لفٹنگ کسے کہتے ہیں؟

جواب: کسی دوست سے سافٹ ویئر کی کاپی لینا اور اسے انسٹال کرنا، سافٹ لفٹنگ کہلاتا ہے۔

-5 کلائنٹ سرور اوور یوز کا کیا مطلب ہے؟

جواب: کلائنٹ سرور اوور یوز (Client Server Overuse) کا مطلب ہے کہ لیے گئے سافٹ ویئر کے لائسنس سے بڑھ کر اس کی کاپیاں انسٹال کرنا۔

-6 ہارڈ ڈسک لوڈنگ کا کیا مطلب ہے؟

جواب: ہارڈ ڈسک لوڈنگ کا مطلب ہے کہ سافٹ ویئر کی غیر مجاز شدہ کاپیاں نئے کمپیوٹر پر انسٹال کرنا یا فروخت کرنا۔

-7 جعل سازی کسے کہتے ہیں؟

جواب: کاپی رائٹ پروگرامز کو نقل اور فروخت کرنا جعل سازی (Counterfeiting) کہلاتا ہے۔

-8 دھوکہ یا غلط استعمال کسے کہتے ہیں؟

جواب: کسی غیر مجاز سرگرمی کے مقصد سے کمپیوٹر کا استعمال دھوکا یا غلط استعمال کہلاتا ہے۔

-9 وارنٹی یا ذمہ داری کسے کہتے ہیں؟

جواب: سافٹ ویئر بنانے کے ساتھ کیے گئے معاہدہ (Agreement) کو وارنٹی یا ذمہ داری کہا جاتا ہے۔

-10 پیٹنٹ کا کیا فنکشن ہے؟

جواب: پیٹنٹ ایک آئیڈیا کی حفاظت کرتا ہے تاکہ اس کا غلط استعمال نہ ہو اور مالک اس کے مکمل حقوق رکھے گا۔

-11 تجارتی راز کو محفوظ کیوں رکھا جاتا ہے؟

جواب: قدر (Value) اور افادیت (Usefulness) کی حفاظت کے لیے ہم تجارتی راز محفوظ رکھتے ہیں۔

for notes, past papers, free test sessions and guess papers visit taleemcity.com

-12 تخریب کاری کسے کہتے ہیں؟ یا حساس معلومات کس طرح سبوتاژ ہوتی ہیں؟

جواب: کمپیوٹر سے دور دراز بیٹھ کر حملہ کیا جا سکتا ہے اس طرح حساس معلومات سبوتاژ ہو جاتی ہیں۔

-13 کرپٹوگرافی یا خفیہ کاری کا کیا مطلب ہے؟

جواب: کرپٹوگرافی یا خفیہ کاری کا مطلب ہے کہ ڈیٹا کو نہ پڑھی جانے والی صورت میں تبدیل کرنا جسے سائیفر ٹیکسٹ (Ciphertext) کہتے ہیں۔ اس کو پڑھنے کے لیے ایک کلید یا کی (Key) کی ضرورت ہوتی ہے۔

-14 پاس ورڈ کا استعمال کیوں کرتے ہیں؟

جواب: پاس ورڈ کو ایک سسٹم میں داخل ہونے کے لیے تصدیق کے طور پر استعمال کیا جاتا ہے۔

-15 سائبر کرائم کسے کہتے ہیں؟

جواب: ایسا جرم جس میں کمپیوٹر نیٹ ورک یا آلات استعمال کیے جاتے ہیں، سائبر کرائم کہلاتا ہے۔

-16 ہیکنگ کسے کہتے ہیں؟

جواب: غیر قانونی طور پر کسی دوسرے کے کمپیوٹر تک رسائی حاصل کرنا ہیکنگ (Hacking) کہلاتا ہے۔

-17 DOS اٹیک کسے کہتے ہیں؟

جواب: DOS اٹیک ایک ایسا سائبر حملہ ہے جس میں ایک مشین یا نیٹ ورک وسائل کو صارفین کے لیے بیکار جاننے کے لیے استعمال کیا جاتا ہے۔

اہم مختصر جوابی سوالات

■ **مندرجہ ذیل مختصر سوالات کے جوابات تحریر کریں۔**

-1 کمپیوٹر سکیورٹی کی وضاحت کریں۔

جواب: کمپیوٹر اور اس کے وسائل کے غیر مجاز استعمال کو روکنے اور اُن کا پتہ لگانے کا عمل کمپیوٹر سکیورٹی کہلاتا ہے۔

-2 کمپیوٹر سکیورٹی کے مقاصد بیان کریں۔

جواب: کمپیوٹر سکیورٹی کے مقاصد درج ذیل ہیں:

(i) ہارڈ ویئر کی چوری یا نقصان کو روکنا (ii) معلومات کی چوری یا نقصان کو روکنا

(iii) خدمت (سروس) میں خلل ڈالنے سے بچانا

-3 سائبر کرائم (Cyber Crime) کی وضاحت کریں۔

جواب: کوئی غیر قانونی (مجرمانہ) سرگرمی جو کمپیوٹر اور انٹرنیٹ کے ذریعے سرانجام دی جائے سائبر کرائم کہلاتا ہے۔

-4 ہیکنگ (Hacking) سے کیا مراد ہے؟

جواب: ایک کمپیوٹر سسٹم یا نیٹ ورک تک قانونی اجازت کے بغیر رسائی ہیکنگ کہلاتا ہے۔

-5 ہیکر کسے کہتے ہیں؟

جواب: ہیکر ایک پروگرام ہوتا ہے جو کمپیوٹر سسٹم یا کسی دوسرے نیٹ ورک میں بغیر اجازت رسائی حاصل کرتا ہے۔

-6 کریکر (Cracker) کی تعریف کریں۔

جواب: کریکر ایک کمپیوٹر پروگرام ہوتا ہے جو کسی نیٹ ورک میں مجرمانہ اور تباہ کن ارادے سے غیر قانونی طور پر رسائی حاصل کرنے کے لیے حفاظتی

نظام کو توڑ دیتا ہے۔

-7 **کمپیوٹر سیکیورٹی تھریٹ کیا ہوتا ہے؟**

جواب: کمپیوٹر سیکیورٹی تھریٹ (Computer Security Threat) ایک ممکنہ خطرہ ہوتا ہے جو سیکیورٹی کی خلاف ورزی کرنے کے خطرات کا فائدہ اٹھا سکتا ہے اور اسی وجہ سے ممکنہ نقصان کا سبب بن سکتا ہے۔

-8 **وائرس کی وضاحت کریں۔**

جواب: وائرس ایک ایسا سافٹ ویئر ہے جو کسی فائل، پروگرام یا کمپیوٹر سسٹم کو متاثر (نقصان) کرتا ہے۔

-9 **ورام (Worm) کیا ہے؟**

جواب: وارم ایک سافٹ ویئر ہے جو کسی انسان کی مدد کے بغیر خود کو ایک کمپیوٹر سے دوسرے کمپیوٹر میں کاپی کرنے کے لیے تیار ہوتا ہے۔

-10 **ایڈویئر (Adware) کیا ہوتا ہے؟**

جواب: ایڈویئر ایک سافٹ ویئر ہے جو خود بخود کمپیوٹر پر اشتہارات ڈسپلے یا ڈاؤن لوڈ کرتا ہے۔

-11 **سپائی ویئر (Spyware) کیا ہوتا ہے؟**

جواب: سپائی ویئر ایک سافٹ ویئر ہے جو یوزر کے علم میں آئے بغیر سسٹم پر انسٹال ہوتا ہے۔

-12 **مالویئر کیا ہوتا ہے؟**

جواب: مالویئر ایسا سافٹ ویئر ہوتا ہے جو مالک کے علم میں لائے بغیر خاص طور پر کسی کمپیوٹر تک رسائی حاصل کرنے یا اس کو خراب کرنے کے لیے ڈیزائن کیا گیا ہے۔

-13 **وائرس پھیلنے کی وجوہات بیان کریں۔**

جواب: وائرس پھیلنے کی وجوہات درج ذیل ہیں:

(i) متاثرہ فلیش ڈرائیو (ii) نیٹ ورک اور انٹرنیٹ

(iii) پائریٹڈ سافٹ ویئر (iv) ای میل دستاویز

-14 **پائریٹڈ سافٹ ویئر کی وضاحت کریں۔**

جواب: کسی کاپی رائٹ سافٹ ویئر کی غیر قانونی کاپی تیار کرنا پائریٹڈ سافٹ ویئر کہلاتا ہے۔

-15 **کمپیوٹر سیکیورٹی سافٹ ویئر کی وضاحت کریں۔**

جواب: کمپیوٹر میں انسٹال ایسے سافٹ ویئر جو کمپیوٹر کو ہیکرز یا وائرس سے محفوظ کرتے ہیں۔

-16 **اینٹی وائرس سے کیا مراد ہے؟**

جواب: یہ ایک ایسا سافٹ ویئر ہے جو خراب سافٹ ویئر کی روک تھام، اس کا پتہ لگانے اور ختم کرنے کے لیے استعمال ہوتا ہے۔

-17 **اینٹی سپائی ویئر (Anti Spyware) کی وضاحت کریں۔**

جواب: ایسا سافٹ ویئر جو کمپیوٹر کو سپائی ویئر سے محفوظ رکھتا ہے۔

-18 **تصدیقی طریقہ کار (Authentication Mechanism) کی وضاحت کریں۔**

جواب: کسی کمپیوٹر کو غیر مجاز استعمال سے محفوظ بنانے کے لیے طریقہ کو تصدیقی طریقہ کار کہتے ہیں۔

-19 آتھورائزڈ ایکسیس (Authorized Access) کی وضاحت کریں۔

جواب: مجاز رسائی (Authorized Access): کسی کمپیوٹر یا کمپیوٹر کی خصوصیات تک قانونی رسائی حاصل کرنے کو مجاز رسائی کہتے ہیں۔

-20 غیر مجاز رسائی (Unauthorized access) کی وضاحت کریں۔

جواب: غیر قانونی طور پر کسی کمپیوٹر یا کمپیوٹر کی خصوصیات تک رسائی حاصل کرنے کو غیر مجاز رسائی کہتے ہیں۔

-21 تصدیق (Authentication) کیا ہوتی ہے؟

جواب: کسی کی شناخت کی تصدیق کرنا جو ڈیٹا، وسائل یا ایپلی کیشنز تک رسائی حاصل کرنا توثیق کہلاتا ہے۔

-22 یوزر نیم (صارف کا نام) کی وضاحت کریں۔

جواب: صارف نام ایک ایسا نام ہے جو کمپیوٹر سسٹم میں کسی کی منفرد شناخت کرتا ہے۔ صارف نام حروف، اعداد یا کچھ خاص حروف کا مجموعہ ہے۔

-23 پاس ورڈ کی وضاحت کریں۔

جواب: پاس ورڈ حروف کا مجموعہ ہوتا ہے۔

-24 لاگ ان کی وضاحت کریں۔

جواب: پاس ورڈ میں حروف کے مجموعہ کو لاگ ان کہا جاتا ہے۔

-25 ذاتی شناختی نمبر (Pin) کیا ہے؟

جواب: ذاتی شناختی نمبر ایک عددی کوڈ ہے جو یوزر کو کمپیوٹر سسٹم تک رسائی حاصل کرنے کے لیے اس کی توثیق کرتا ہے۔

-26 ایکسیس کارڈ سے کیا مراد ہے؟

جواب: یہ ایک ایسا طریقہ کار ہے جو کمپیوٹر یا اس کے ذرائع (وسائل) تک رسائی حاصل کرنا ہے۔

اہم کثیر الانتخابی سوالات

■ **مندرجہ ذیل کثیر الانتخابی سوالات کے چار ممکنہ جوابات دیے گئے ہیں۔ درست جواب پر (✓) کا نشان لگائیں۔**

-1 ایک مجرمانہ فعل جو کمپیوٹر اور انٹرنیٹ کے ذریعہ انجام دیا جاتا ہے اسے ______ کا نام دیا جاتا ہے۔

(A) سائبر سپیس (B) سائبر کرائم (C) کرائم (D) کمپیوٹر کرائم

-2 ایک سافٹ ویئر جو خود بخود اپنے آپ کو نقل کرتا ہے کہلاتا ہے۔

(A) وائرس (B) ایڈویئر (Adware) (C) وارم (Warm) (D) سپائی ویئر (Spyware)

-3 ایک ایسا سافٹ ویئر جو یوزر کی براؤزنگ (browsing) کی عادات کا پتہ لگاتا ہے اسے ______ کہتے ہیں۔

(A) وائرس (Virus) (B) وارم (Worm) (C) ایڈویئر (Adware) (D) ہیکر (Hacker)

-4 ایک پروگرام جو کمپیوٹر سسٹم کو توڑتا ہے، اسے کہتے ہیں۔

(A) کریکر (Cracker) (B) بریکر (Breaker) (C) ہاکر (Hawker) (D) ہیکر (Hacker)