یونٹ 4 ڈیٹا اور رازداری کا معاملہ

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 تعلّم (Students Learning Outcomes)

1- سکیورٹی سے متعلق اخلاقی مسائل:

- ڈیٹا کی سکیورٹی 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 تجربہ 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۔
- فریکوینسی تجزیہ (Frquency 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:

- کرپٹوگراف کی (Crypptographic 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 Servic)DOS حملہ کس طرح ہوتا ہے بیان کرنا۔

تعارف:

آج کل کمپیوٹر ہر جگہ موجود ہیں اور تقریباً ہر عمر کے لوگ اس کو استعمال کرتے ہیں۔ اکثر ہمیں کمپیوٹر کو اپنی ذاتی معلومات فراہم کرنے کی ضرورت پیش آتی ہے۔ مثال کے طور پر ای میل اکاؤنٹ بناتے ہوئے، آن لائن خریداری کرتے ہیں، ایک ہسپتال کا دورہ اور سکول میں داخلہ لیتے ہوئے اور ہم یہ خیال کرتے ہیں کہ ہماری فراہم کردہ معلومات کسی کو نہیں بتائی جائیں گی۔ ضرر پہنچانے والے صارفین سے ڈیٹا کی حفاظت کرنا ڈیٹا یا معلومات کی رازداری کہلاتی ہے۔

4.1 سیکیورٹی سے متعلق اخلاقی مسائل:

4.1.1 سیکیورٹی سے متعلق اخلاقی مسائل کو سمجھنا:

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 سیکیورٹی (حفاظتی) کے چند مسائل درج ذیل ہیں:

- رازداری اور پوشیدگی
- دھوکہ دہی اور غلط استعمال
- پیٹنٹ (Pattent)
- کاپی رائٹ (Copyright)
- تجارتی راز
- تخریب کاری (Sabotage)

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 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 لائیسنس، 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۔

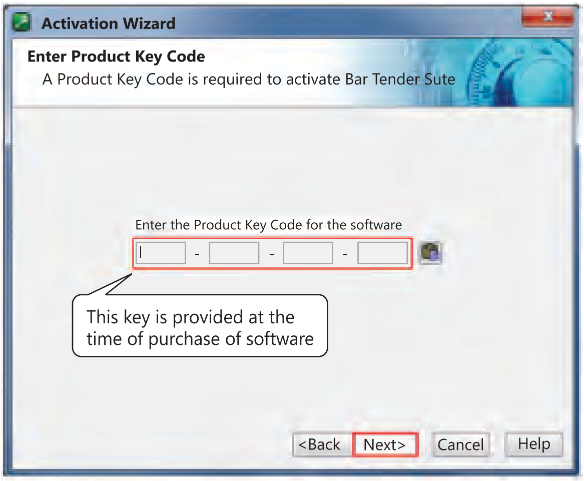
پائیریسی (Piracy) (غیر قانونی کاپی رائٹ):

پائیریسی کا مطلب غیر قانونی نقلیں تیار کرنا ہے۔ کتاب، شاعری، سوفٹ ویئر، فلم، مصوری، گھر کا نقشہ تعمیر یا کسی ایسے کام کی خلافِ قانون نقل کرنا جو ازروئے قانون ممنوع ہے۔

کیا آپ جانتے ہیں؟

Open source software میں کوئی کاپی رائٹ کے تحفظات نہیں ہوتے لہٰذا ہم source code کاپی کر سکتے ہیں اس میں ترمیم کر سکتے ہیں۔ اور اسے فروخت بھی کر سکتے ہیں۔

سافٹ ویئر پائریسی کسی سافٹ ویئر کی غیر قانونی کاپی، تقسیم یا استعمال ہے۔ کچھ سافٹ ویئر کمپنیاں سافٹ ویئر کو خفیہ متن کے ساتھ فروخت کرتی ہیں۔ جسے اس سافٹ ویئر کی (Key) کہتے ہیں۔ یہ کی (Key) صرف ان لوگوں کو فراہم کی جاتی ہے جو اس سافٹ ویئر کو خریدتے ہیں۔ اس کی مدد سے غیر قانونی انسٹال کرنے سے روکا جاتا ہے۔ جیسا کہ شکل 4.1 میں دکھایا گیا ہے۔ کچھ لوگ غیر قانونی ذرائع استعمال کر کے اس مخصوص کی (Key) تلاش کر لیتے ہیں، اسے کی (Key) توڑنا کہتے ہیں۔



Enter Product Key Code
A Product Key Code is required to activate Bar Tender Sute

Enter the Product Key Code for the software

This key is provided at the time of purchase of software

شکل 4-1 سوفٹ ویئر ایکٹیویٹ کرنا

سافٹ ویئر پائیریسی کی اقسام میں شامل ہیں:

سافٹ لفٹنگ (Softlifting)

کسی دوسرے سے ایپلیکیشن سافٹ ویئر کی کاپی لے کر انسٹال کرنا

کلائنٹ سرور اوور یوز (Client-Server-Over use)

حاصل کردہ لائسنس کے مقابلے سافٹ ویئر کی مزید کاپیاں انسٹال کرنا

ہارڈ ڈسک لوڈنگ (Hard disk-loading)

تجدید شدہ یا نئے کمپیوٹر پر غیر مجاز شدہ سافٹ ویئر کی کاپیاں انسٹال اور فروخت کرنا۔

جعل سازی (Counterfeiting)

سافٹ ویئر کی نقلیں تیار کرنے اور بیچنے کے بھی کاپی رائٹ ہوتے ہیں۔

آن لائن پائریسی (Online Piracy)

آن لائین پائیریسی میں عموماً غیر قانونی سافٹ ویئرز ڈاؤن لوڈ کرنا شامل ہے۔ سافٹ ویئرز کمپنیاں سافٹ ویئر پائیریسی کے خلاف جنگ کر رہی ہیں۔ عدالتیں سافٹ ویئر کے تحفظ کے لیے قوانین بھی بنا رہی ہیں۔

دھوکا 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 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۔

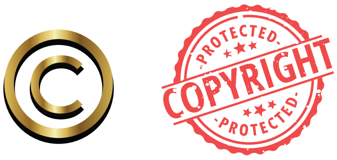
شکل 4-2

شکل 4-3

پیٹنٹ (Patent)

پیٹنٹ کسی آئیڈیا (Idea) 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۔

مثال: اگر آپ طبی میدان میں تحقیق کر رہے ہیں اور کسی مخصوص بیماری کا علاج کرنے کے لیے ایک نیا آئیڈیا پیش کرتے ہیں تو بعض دواسازی کمپنیاں آپ کے آئیڈیا کی بنیاد پر ادویات تیار کر سکتی ہیں۔ اخلاقی طور پر اُن کو آپ کے آئیڈیا کی بنیاد پر ادویات بنانے سے پہلے آپ کی اجازت لینی چاہیے انھیں دوا کی فروخت پر بھی آپ کو ایک خاص رقم ادا کرنی چاہیے۔ اس کے لیے آپ کو ایک پیٹنٹ حاصل کرنا ہوگا۔



شکل 4-4 کاپی رائٹ کا نشان

کاپی رائٹ قانون:

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۔ عام طور پر اگر کوئی چیز کاپی رائٹ کے تحت محفوظ ہے تو ہم اس میں ایک کاپی رائٹ کا نشان رکھتے ہیں جیسا کہ شکل 4.4 میں دکھایا گیا ہے۔

مثلاً: جو کتاب آپ پڑھ رہے ہیں اُس کے کاپی رائٹ کے حقوق محفوظ ہیں۔ اس کا مطلب یہ بھی ہوا کہ ہم اس کی کاپی نہیں بنا سکتے۔ کاپی رائیٹ ڈیٹا کے غلط استعمال سے روکتا ہے۔ ڈیٹا میں کمپیوٹر پروگرام، ڈاکومینٹس یا اسی طرح کا ملتا جلتا مواد آتا ہے۔

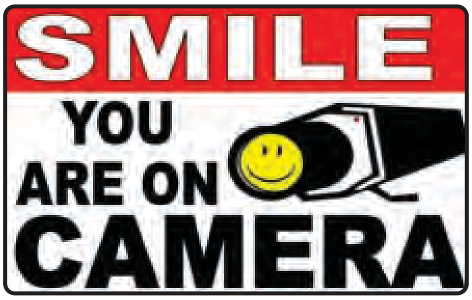
تجارتی راز:

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۔

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۔

4.1.2 دوسروں کی رازداری کی حفاظت:

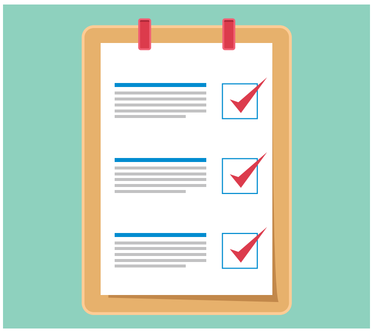


شکل 4-5

کیا آپ نے کبھی ”کیمرہ آپ کو دیکھ رہا ہے“ سڑکوں پہ لگے بورڈ کا مشاہدہ کیا ہے جیسا کہ شکل 4.5 میں دکھایا گیا ہے۔ 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 (Speed Cameras) 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۔

کیا آپ جانتے ہیں؟

سی سی ٹی وی (CCTV) کلوز سرکٹ ٹیلی وژن کے لیے ہے۔



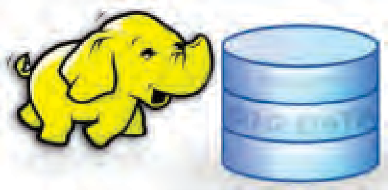
شکل 4-6

زیادہ تر ویب سائٹس نے اپنی رازداری کی پالیسیوں (4.6 شکل) کی نشاندہی کی ہوتی ہے جو یہ بتاتی ہیں کہ وہ آپ سے متعلق اور آپ کے کمپیوٹر کی کونسی معلومات اکٹھی کرتی ہیں اور ان معلومات کا اشتراک وہ کس کے ساتھ کریں گی۔ لوگ ان پالیسیوں کو نظر انداز کرتے ہیں۔ زیادہ تر صارفین غلطی سے 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 گی۔

4.2 ڈیٹا رازداری کی اہمیت:

4.2.1 ڈیٹا کے بڑے مجموعے سے رازداری کے متاثر ہونے کے خدشات:

کمپیوٹرائزڈ نظام کی وجہ سے بہت سے ادارے ہمارے ڈیٹا کو محفوظ رکھتے ہیں۔ آپ کی سوچ سے بڑھ کر آپ کی معلومات رکھنے والے لوگ اور تنظیمیں ہوسکتی ہیں۔



شکل 4-7

مثال کے طور پر:

- ہسپتال کے پاس آپ کی پیدائش کا ریکارڈ ہوسکتا ہے۔
- نادرا کے پاس آپ کے خاندان کی معلومات ہے۔
- آپ کے سکول کے پاس آپ کا ریکارڈ ہے۔
- ثانوی و اعلیٰ ثانوی تعلیمی بورڈ (BISE) کے پاس آپ کا ریکارڈ ہے۔
- پاسپورٹ آفس کے پاس اگر آپ کا پاسپورٹ ہے۔
- ای میل سروس فراہم کرنے والوں کے پاس اگر آپ کا ای میل اکاؤنٹ ہے۔
- آن لائن سوشل نیٹ ورکنگ ویب سائٹس وغیرہ۔

بہت سی کمپنیوں کو آپ کے نام، ایڈریس اور آپ کی زندگی کے بارے میں دیگر بنیادی حقائق سے کہیں زیادہ دلچسپی ہوتی ہے۔ وہ جاننا چاہتی ہیں کہ آپ نے کہاں سفر کیا ہے؟ آپ کس قسم کے کپڑے پہنتے ہیں؟ آپ کب بیمار ہوئے؟ اگر آپ ایک شے خریدتے ہیں تو کیا آپ اس چیز کے ساتھ کچھ اور خریدتے ہیں یا نہیں۔ ان سوالات کے جوابات فیصلہ سازی میں معاون ہوتے ہیں۔

مثال: اگر آپ آلو کے چپس کا پیکٹ خریدتے ہیں تو عام طور پر اس کے ساتھ ایک مشروب بھی خریدتے ہیں۔ یہ معلومات ایک شاپنگ مال کے لیے مفید ہے تاکہ ان کی فروخت بڑھانے کے لیے دونوں ”آلو کی چپس اور مشروبات“ پر آفر دی جاسکے۔ لہٰذا معلومات کا ایک حصہ کسی ایک جگہ سے دوسری جگہ کسی کو اطلاع دیے بغیر منتقل ہوسکتا ہے، ایسا ڈیٹا کے بڑے مجموعے کی وجہ سے ہے۔

DATA BROKER

شکل 4-8

کیا آپ جانتے ہیں؟

بعض کمپنیاں جنھیں ڈیٹا بروکرز (Data Brokers) کہا جاتا ہے، صرف صارفین کی معلومات جمع کرنے، مجموعہ کرنے، خرید و فروخت کرنے کے لیے موجود ہیں۔

4.2.2 کمپیوٹنگ سسٹم کو استعمال کرنے سے پیدا ہونے والے ذاتی رازداری اور حفاظتی خدشات کا تجزیہ

انٹرنیٹ کی آمد کے ساتھ، ہمارے کمپیوٹرز اب تن تنہا کام کرنے والے نہیں رہے۔ اصل میں اب وہ دنیا میں لاکھوں دوسرے کمپیوٹرز کے ساتھ منسلک ہیں اس رابطے کی وجہ سے بہت سے سیکورٹی خدشات بھی پیدا ہوتے ہیں۔ بنیادی طور پر ہم مندرجہ ذیل تین پہلوؤں کے مطابق اپنے ڈیٹا کو محفوظ رکھنا چاہتے ہیں۔

-1 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۔

-2 صداقت (Integrity)

ہم ڈیٹا کو درست رکھنا چاہتے ہیں۔ مثال کے طور پر ہم یہ نہیں چاہتے کہ ہماری بینک کی ویب سائٹس ہمارے بینک بیلنس کو اکاؤنٹ میں موجود رقم سے کم ظاہر کریں۔

-3 دستیابی (Availability)

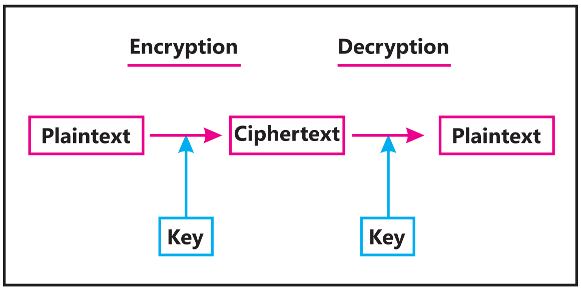
اس سے مراد یہ ہے کہ جب چاہیں اپنے ڈیٹا پر رسائی حاصل کر سکیں۔ کیونکہ اگر فروخت کے وقت ڈیٹا میسر نہ ہو تو پھر کچھ دوسری صورتوں میں یہ بیکار ہو جاتا ہے۔ یہ تمام پہلو کمپیوٹرائزڈ نظام میں ڈیٹا بیس کی پروسیسنگ، اسٹوریج اور ٹرانسمیشن کے دوران بہت اہم ہیں۔ کمپیوٹیشن (Computation) کسی بھی قسم کی معلومات کی پروسیسنگ کے لیے عام اصطلاح ہے جس کی ریاضی میں نمائندگی کی جا سکتی ہے مثال کے طور پر آپ کی نویں کلاس کے گریڈ کو آپ کے ہر مضمون میں آپ کے حاصل نمبرز کے مطابق شمار کیا جائے گا۔ ہر فرد کی زندگی میں کمپیوٹنگ سسٹم کا استعمال روز افروں ہے جس کی وجہ سے رازداری کے بہت خدشات پیدا ہو رہے 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۔ کمپنیاں ویب سرفرز (Web surfers) کے دماغ کو پڑھنا چاہتی ہیں اور کبھی کبھی وہ معلومات کے کچھ حصوں کو ویب سرفرز کے ساتھ ذخیرہ کرتے ہیں جسے کوکیز (Cookies) کہتے ہیں۔ کوکیز کا استعمال کرتے ہوئے کمپنیاں ذاتی معلومات کو خریدنے اور اکٹھی کرنے کے قابل ہوتی ہیں۔ وہ ان معلومات کو مارکیٹنگ کے لیے استعمال کرتی ہیں۔ اس عمل کو رازداری پر حملہ سمجھا جاتا ہے۔

شکل 4-9

4.3 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 اسے پڑھ سکتے ہیں۔ ان کوڈنگ کا مطلب ڈیٹا کو نہ پڑھے جا سکنے والی شکل میں تبدیل کرنا ہے۔ جیسے سائفر ٹیکسٹ (Ciphertext) کہتے ہیں۔ ایک خفیہ کوڈ جسے کلید یا کی (Key) کہا جاتا ہے، ڈیٹا کو پڑھنے کے لیے ضروری ہوتا ہے جیسا کہ شکل 4.10 میں دکھایا گیا ہے۔ کی (Key) ایک پاس ورڈ کی طرح ہوتی ہے۔

ماضی میں پیغامات لوگوں کی مدد سے دوردراز پہنچائے جاتے تھے تو اس وقت کے بادشاہ اور حکمران اپنے پیغامات کو اینکرپٹ (Encrypt) کر کے اپنے اتحادیوں کو بھیجتے تھے۔ یوں سے پیغامات کی رازداری کو چوری ہونے کی صورت سے محفوظ کیا جاتا تھا۔



شکل 4-10

کمپیوٹر ماہر جو ڈیٹا چوری کر سکتا ہے (جب یہ ڈیٹا ایک مقام سے دوسرے مقام پر بھیجا جائے) اسے ہیکر (Hacker) کہا جاتا ہے۔ خفیہ کاری ہمارے ڈیٹا کو ہیکرز سے بچانے میں مدد کرتی ہے۔

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 حرف کی جگہ پر اگلا حرف ڈال دیا جائے مثلاً 'a' بن جائے گا 'b' 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۔

سرگرمی: 4.2

اگر آپ اپنی تحریر کو آیئنے 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 چاہیئے جیسا کہ آپ اپنی عام تحریر کو آئینے میں دیکھتے ہیں۔ اِسی طرح آپ مختلف الفاظ لکھیں، یا کسی کو ایک نوٹ لکھیں پھر اسے الٹا کریں اور انھیں بھیج دیں۔

4.3.1 روزمرہ زندگی میں انٹرنیٹ پر خفیہ کاری کی اہمیت:

ڈیٹا کو سیکورٹی فراہم کرنے کے لیے خفیہ کاری 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:

INTERNET BANKING

شکل 11-4

1- ہیکرز سے تحفظ

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

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۔

شکل 11-4

-3 خفیہ کاری آلات میں ڈیٹا کی حفاظت کرتی ہے

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 محظوظ کرتے وقت یہاں تک 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۔

4.3.2 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 دیئے جاتے ہیں۔ یہ متبادل عمل ایک مقررہ وضاحتی نظام کی مدد سے کیا جاتا ہے۔ ذیل میں ہم دو عمومی طور پر استعمال ہونے والے متبادل سازی کے طریقوں کی بات کرتے ہیں۔

4.3.2.1 سیزر سائیفر (Caeser Cipher)

سیزر ایک رومن سیاست دان اور فوجی جنرل تھا جس نے رومن سلطنت کے عروج میں اہم کردار ادا کیا۔ سیزر نے اپنے فوجیوں اور جرنیلوں کو پیغامات بھیجنے کے لیے ایک خفیہ کاری کا طریقہ استعمال کیا۔ اس لیے اس طریقے کو سیزر سائیفر کہا جاتا ہے۔ اس طریقے میں ہم ہر حروفِ تہجی (Alphabets) کو تحریر کرتے وقت دوسرے حرف سے تبدیل کر دیتے ہیں۔ حروف کی ترتیب میں اصل حروف تہجی کے بائیں یا دائیں کے لیے کچھ طے شدہ نمبرز ہوتے ہیں۔

مثال 1: معیاری انگریزی حروفِ تہجی کے ''تین حروف دائیں جانب متبادل'' سے ہمیں مندرجہ ذیل نتائج حاصل ہوتے ہیں۔

ابتدائی حروف: ABCDEFGHIJKLMNOPQRSTUVWXYZ

خفیہ کاری حروف: DEFDEFGHIJKLMNOPQRSTUVWABC

اس متبادل طریقے کے تحت سادہ عبارت "PAKISTAN" خفیہ کاری کی صورت میں "QBLJTUBO" میں تبدیل ہو جائے گی۔

مثال 2: معیاری انگریزی حروفِ 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۔

سرگرمی: 4.3

تین حروف متبادل (three-character sub) کو سادہ عبارت "PAKISTAN" کے بائیں طرف استعمال کرتے ہوئے خفیہ کاری میں تبدیل کریں۔

4.3.2.2 وگنیر سائیفر (Vigenere Cipher)

وگنیر 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 وگنیر سائیفر ٹیبل کہتے ہیں۔

وگنیر سائیفر ٹیبل (Vigenere Cipher Table)

اس ٹیبل کو ٹیبل (4.1) میں دکھایا گیا ہے یہ ٹیبل چھبیس قطاروں اور چھبیس کالموں پر مشتمل ہے۔ جہاں پہلی قطار میں اصل A-Z حروف تہجی ہیں۔ باقی ہر ایک 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	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

ٹیبل 4-1

وگینیر سائیفر طریقہ:

اس طریقے میں 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 وگینیر ٹیبل کے کالم میں تلاش کرتے ہیں (ٹیبل 4.1) 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 (ٹیبل 4.1)۔ 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 ٹیبل (4.1) میں ملاحظہ 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 (4.2) 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

ٹیبل 4.2

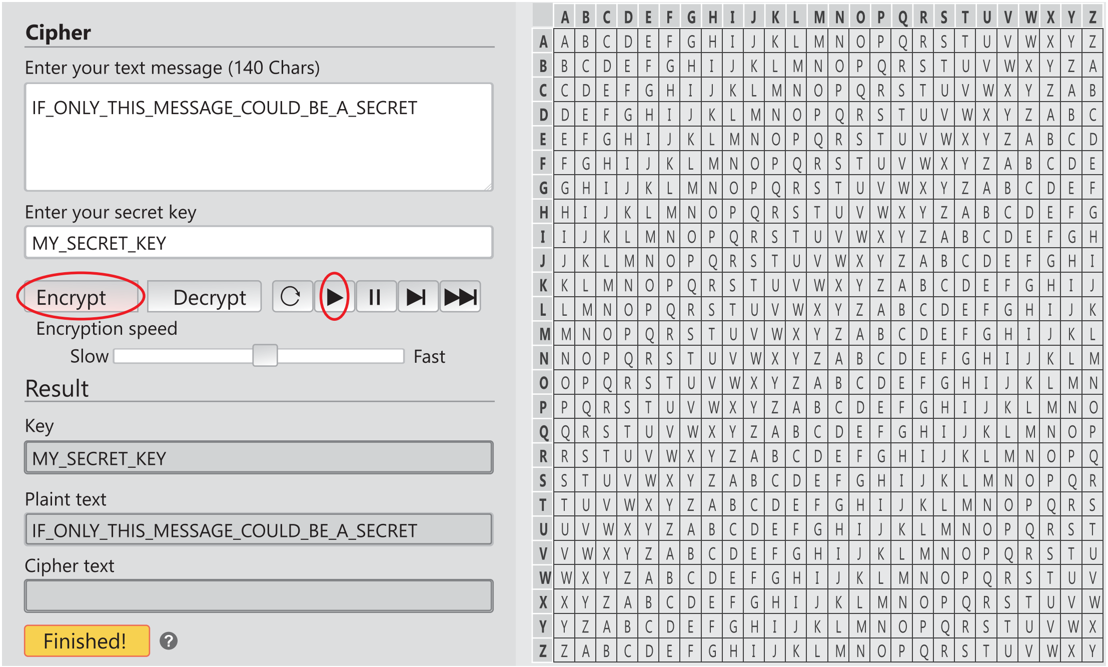
اہم نوٹ: اگر کلید کے حروف کی تعداد عبارت کے حروف سے کم ہو تو ہم کلید کے حروف کو شروع سے دوبارہ لکھیں گے۔ مثال کے طور پر لفظ "PAKISTAN" جس کے آٹھ حروف میں کو کلید (Key) "BEAUTY" جس کے چھے خطوط میں سے خفیہ کاری میں تبدیل کرنا چاہتے ہیں تو ہم کلیدی حروف کو دیئے گئے لفظ میں لمبائی میں برابر کرنے کے لئے دوبارہ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

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۔

4.3.3 وگینیر سائیفر ویجیٹ (Vigenere Cipher Widget) کا استعمال:

ویب سائٹ http://stdio.code.org/s/vigenece/stage/1/puzzle/1 پر ایک ویجیٹ دستیاب ہے اسے وگینیر سائیفر خفیہ کاری ویجیٹ کہا جاتا ہے۔ یہ دی گئی کلید کے مطابق وگینیر سائیفر کا استعمال کرتے ہوئے سادہ عبارت کی خفیہ کاری اور decryption کو حرکت پذیری (animation) کی صورت میں دکھاتی ہے۔ اس ویجیٹ کی تصاویر کو شکل 4.13 میں دکھایا گیا ہے۔ آپ اوپر بائیں کونے پر عبارت لکھ سکتے ہیں اور خفیہ کاری کے لیے ایک کلید (Key) فراہم کرسکتے ہیں۔ خفیہ کاری کے بٹن کو دبائیں اور اس کے بعد خفیہ کاری کی حرکت پذیری کے لیے کلک کریں۔ دونوں بٹنوں پر سُرخ دائرے کا نشان ہے۔ جیسا شکل 4.13 میں دکھایا گیا ہے۔ اسی طرح اصل پیغام دیکھنے کے لیے سائیفر عبارت کو منسوخ کرسکتے ہیں۔



Cipher

Enter your text message (140 Chars)

IF_ONLY_THIS_MESSAGE_COULD_BE_A_SECRET

Enter your secret key

MY_SECRET_KEY

Encryption speed

Result

Key

MY_SECRET_KEY

Plaint text

IF_ONLY_THIS_MESSAGE_COULD_BE_A_SECRET

Cipher text

	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

شکل 4-13

ایک پیغام ڈیکرپٹ (Decrypt) کرنے کا عمل:

پیغام ڈیکرپٹ کرنے کے لیے وگینیر 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۔

کیا آپ جانتے ہیں؟

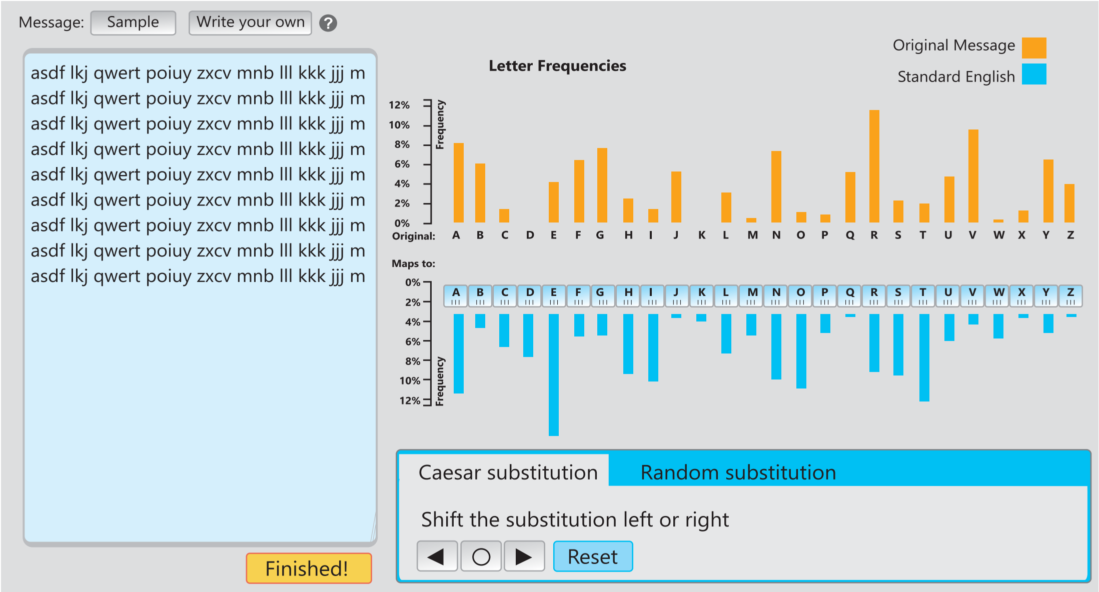
گائس جولیس سیزر 13 جولائی 100 قبل مسیح، روم (اٹلی) میں پیدا ہوا اور 15 مارچ 44 قبل مسیح میں قتل کیا گیا تھا اس کے مشہور اقوال یہ ہیں:

1- تجربہ ہر چیز کا استاد ہے۔
2- مرد آزادانہ طور پر اس بات پر یقین رکھتے ہیں جس کی وہ خواہش رکھتے ہیں۔

4.3.4 فریکوینسی تجزیہ استعمال کرتے ہوئے بے ترتیب متبادل کے ساتھ خفیہ کاری:

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 کیلئے ویجیٹ کو دیکھ سکتے ہیں۔ اس کی تصاویر شکل 4.7 میں دیکھی جا سکتی ہیں۔



asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m

Shift the substitution left or right

Message:
Sample
Write your own
?
Letter Frequencies
Original Message
Standard English
Frequency
12%
10%
8%
6%
4%
2%
0%
Original:
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
Maps to:
Caesar substitution
Random substitution
◀ ○ ▶
Reset
Finished!

شکل 4-14

سرگرمی: 4.5

پیغام ڈراپ ڈاؤن سے نمونہ پیغام داؤن 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 حروفِ 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 حروفِ تہجی کے نیلے خطوط کو براہِ 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 ورزن میں آپ گراف ساتھ مزید بات جیت کریں گے جو خط کی تعداد دکھائے گا۔

کیا آپ جانتے ہیں؟

'E' انگریزی زبان میں سب سے زیادہ استعمال کیا جانے والا حرف ہے۔

آپ کے خفیہ کردہ پیغام میں سب سے زیادہ استعمال ہونے والا 'E' کے ساتھ تبدیل ہوسکتا ہے۔ لیکن ایسا نہیں بھی ہوسکتا ہے۔ آپ کو تھوڑا اندازہ لگانا پڑے گا۔ Cryptanalysis سائیفر پیغام میں حروف یا گروپوں کی فریکوینسی کا مطالعہ ہے یہ طریقہ کار کلاسیکل سائیفر کو توڑنے کے لیے امداد کے طور پر استعمال کیا جاتا ہے۔

4.3.5 متبادل سائیفر کے نقائص:

تمام متبادل سائیفر میں یہ سب سے آسان ہے کیونکہ سائیفر حروفِ تہجی محض حروفِ 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۔

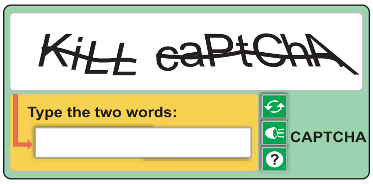
سادہ متبادل سائیفر کے ساتھ ایک اور اہم مسئلہ یہ ہے کہ حروف کی تعداد بالکل ماسکڈ (Masked) نہیں ہوتی۔

4.4 کیز اور پاس ورڈ کے ساتھ خفیہ کاری:

4.4.1 کرپٹوگرافک (Cryptographic) کیز اور پاس ورڈز کے درمیان تعلقات:

شکل 4-15

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 سیکیورٹی 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 جاسکتا 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 کرسکتا ہے۔



ہم ایک ایسا پروگرام تحریر کر سکتے ہیں جو کسی ویب سائٹ تک رسائی حاصل کرسکتا ہے اور اسے ایک پاس ورڈ بھی فراہم کرے۔ اگر یہ پروگرام ایک طویل عرصے تک مختلف پاسورڈ فراہم کرتا رہے تو پاس ورڈ کو ہیک (Hack) کیا جا سکتا ہے۔ اس کے علاوہ ایک پروگرام بار بار غیر ضروری ڈیٹا ایک فارم میں داخل کرسکتا ہے اس صورت حال سے بچنے کے لیے کمپیوٹر کے بجائے صرف انسان ہی اس سسٹم کا استعمال کر سکتے ہیں۔ لہٰذا جب بھی ویب سائٹ پر فارم کو ڈیٹا دیا جاتا ہے تو وہاں ایک تصویر دکھائی جاتی ہے اور آپ کو اس تصویر کو پڑھنے اور فیلڈ (Field) میں لکھنے کے لیے کہا جاتا ہے۔ اس تصویر میں بے ترتیب عبارت شامل ہوتی ہے جسے ایک انسان ہی پڑھ سکتا ہے لیکن مشین کے لیے آسان نہیں ہوتا۔ کچھ سرور کمپیوٹر (Server computer) ہمارے کمپیوٹر پر پاس ورڈ کو محفوظ کرتے ہیں جب ہم انھیں پہلی بار استعمال کرتے ہیں بعد میں استعمال کے لیے ہماری طرف سے بغیر کسی عمل کے اس پاس ورڈ کو استعمال کیا جاتا ہے۔

4.4.2 اچھے پاس ورڈ کی خصوصیات:

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 ہوسکتی ہیں:

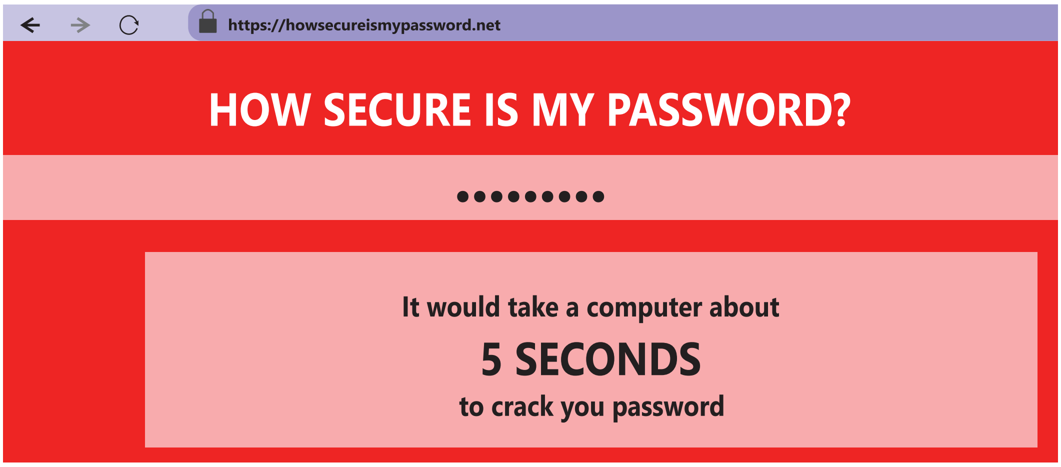
- یہ کم سے کم آٹھ حروف پر مشتمل ہو۔
- یہ آپ کے یوزر نیم (Username)، عرف، بچے کا نام یا کمپنی کے نام پر مشتمل نہ ہو۔
- یہ مکمل لفظ پر مشتمل نہ ہو۔
- یہ گزشتہ پاس ورڈز سے نمایاں طور پر مختلف ہو۔
- یہ بڑے حروف، چھوٹے حروف، نمبر اور علامات پر مشتمل ہو۔

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۔



https://howsecureismypassword.net

HOW SECURE IS MY PASSWORD?

●●●●●●●●●●

It would take a computer about

5 SECONDS

to crack you password

4.5 سائبر کرائم (Cyber Crime):

انٹرنیٹ مواصلات کے لیے حیرت انگیز ذریعہ ہے۔ یہ صارفین کے طویل فاصلے پر ہونے کے باوجود فوری رابطہ استوار کرتا ہے۔ بدقسمتی سے یہ جرائم پیشہ افراد کے لیے بھی مددگار ثابت ہو سکتا ہے۔ ایک جرم جس میں کمپیوٹر نیٹ ورک یا آلات استعمال کیا جاتا ہے اسے سائبر کرائم کہا جاتا ہے۔ مثال کے طور پر:

شناخت کی چوری:

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

ٹرانزیکشن فراڈ:

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

BIG
PRIZE
WINNER

شکل 4-16

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۔

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 تاکہ 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 اِس فراڈ کا شکار ہو جاتے ہیں۔

ہیکنگ (Hacking)

شکل 4-17

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 (4.17) میں دکھایا گیا ہے۔

پائریسی (Piracy)

پائریسی بھی سائبر جرم کی ایک قسم ہے پائریسی کی تفصیلات سیکشن 4.1.1 میں بیان کی جا چکی ہے۔

کیا آپ جانتے ہیں؟

سائبر کرائم کے خلاف نیشنل رسپونس سینٹر (National Response Centre) پاکستان کی قانون نافذ کرنے والی ایجنسی ہے جو سائبر کرائم سے لڑنے کے لیے وقف ہے۔ یہ ایف آئی اے (وفاقی تحقیقاتی ایجنسی) کے تحت کام کر رہی ہے۔ اور اس کی ویب سائیٹ www.nrse.gov.pk پر دستیاب ہے۔

Not secure | www.nr3c.gov.pk
NATIONAL RESPONSE CENTRE FOR CYBER CRIME
CYBER SCOUTS
DEVOTED VOLUNTEERS TO HELP
PAKISTAN FIGHT TECHNOLOGY
DRIVEN CRIME
CYBER SCOUT

سرگرمی: 4.7

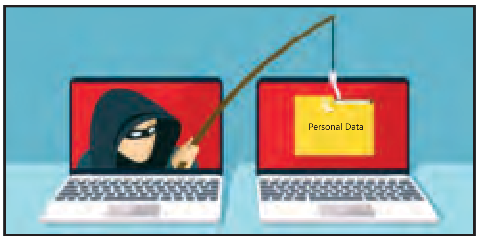
سائبر کرائم کی اقسام httpL//nrse.gov.pk پر تلاش کریں اور ہر ایک کے بارے میں نوٹ لکھیں۔ اساتذہ طالب علموں کے گروپ بنا سکتے ہیں اور ہر گروپ کو ہر قسم پر چارٹ بنانے کے لیے کہہ سکتے ہیں۔

4.5.1 فشنگ اٹیک (Phishing Attack) کی خصوصیات

فشنگ، پاس ورڈ اور کریڈٹ کارڈ کی تفصیلات جیسی حساس معلومات ای میل کے ذریعے حاصل کرنے کی ایک جعل ساز کوشش ہے۔

فشنگ ای میل کی خصوصیات:

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 ہے۔



شکل 4-17

مثال:

- 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- نظرثانی 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۔ ہو سکتا ہے کہ اس ای میل میں کچھ لنک ہوں جن کا آپ کے

سکول کے ساتھ کوئی 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 دھوکہ دینے والی ای میل اسطرح لگاتے ہیں کہ وہ حقیقی ای میل لگے۔

5- یہ ذاتی مالی 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 جاسکتی ہیں۔

فشنگ ویب سائٹ کی خوبیاں

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

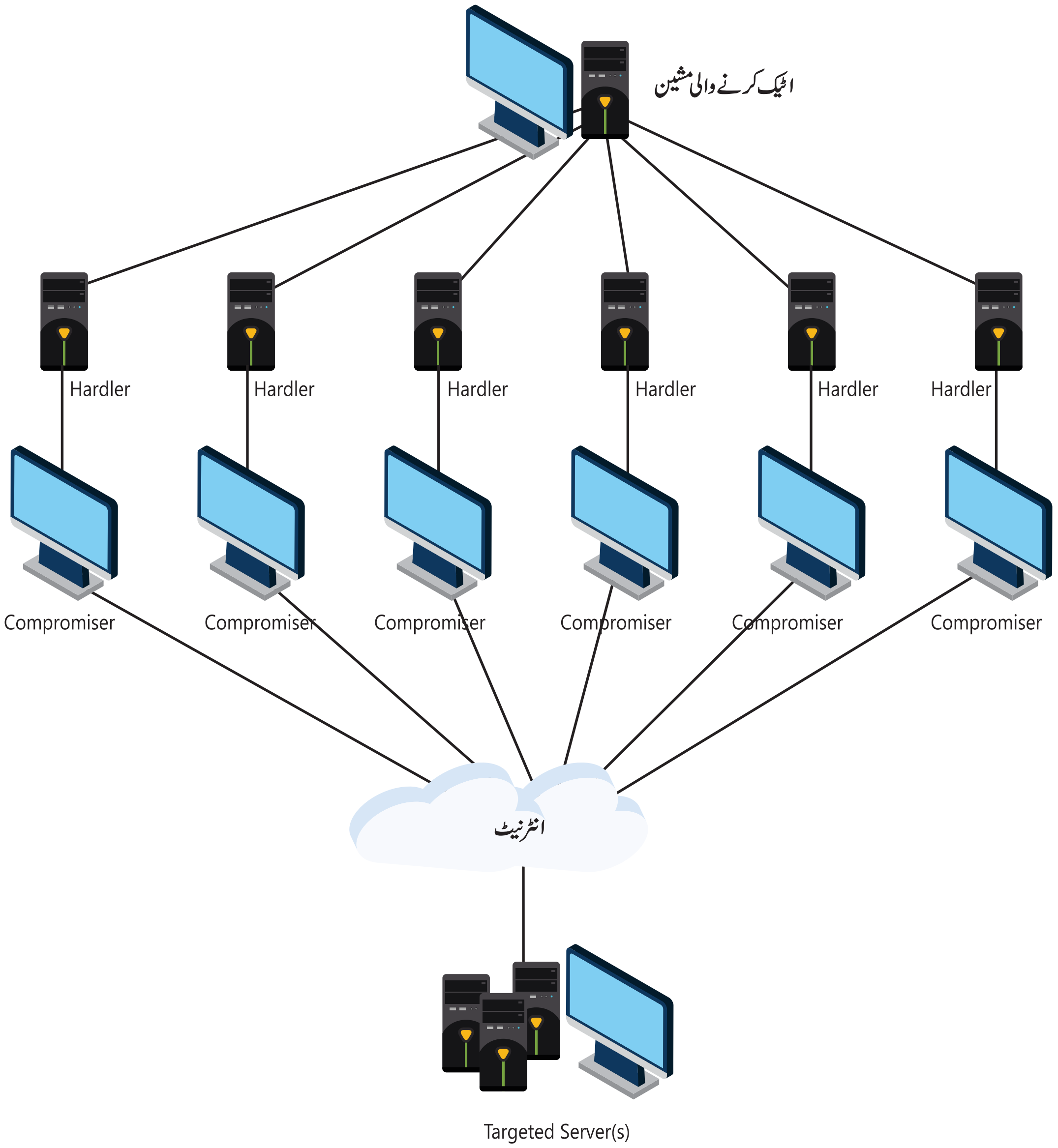
2- یہ اصل ویب سائٹ کے لنک پر مشتمل ہوسکتی ہے۔ جیسا کہ ہم سے رابطہ کریں، رازداری یا دستبرداری کا اعلان جس سے دیکھنے والے کو دھوکا ہو سکتا ہے۔

3- یہ اصل ویب سائٹ پر استعمال ہونے والے نام استعمال کرسکتی 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۔

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 کرسکیں گے۔ اس قسم کے حملے کو شکل (4.19) میں دکھایا گیا ہے۔ 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۔


اٹیک کرنے والی مشین
Hardler
Hardler
Hardler
Hardler
Hardler
Hardler
Compromiser
Compromiser
Compromiser
Compromiser
Compromiser
Compromiser
انٹرنیٹ
Targeted Server(s)

شکل 4-19 ڈاس (DoS) اٹیک

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 کروا سکتے ہیں۔

خلاصہ

- ہمیں انٹرنیٹ پر ڈیٹا بھیجتے ہوئے محتاط رہنے کی ضرورت ہوتی ہے۔
- ہر وہ تنظیم جس کو ڈیٹا منتقل کیا جاتا ہے ڈیٹا کی رازداری اور تحفظ اُس کی ذمہ داری ہے۔
- پائریسی (Piracy) کا مطلب ہے مالک کی اجازت کے بغیر سافٹ ویئر کی غیر قانونی اور غیر مجاز شدہ نقل۔
- کسی دوست سے سافٹ ویئر کی کاپی لینا اور اسے انسٹال کرنا سافٹ لفٹنگ کہلاتا ہے۔
- 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۔
- ہارڈ ڈسک لوڈنگ کا مطلب ہے کہ سافٹ ویئر کی غیر مجاز شدہ کاپیاں نئے کمپیوٹر پر انسٹال کرنا یا فروخت کرنا۔
- کاپی رائٹ پروگرامز کو نقل اور فروخت کرنا جعل سازی (Counterfeiting) کہلاتا ہے۔
- کسی غیر مجاز سرگرمی کے مقصد سے کمپیوٹر کا استعمال دھوکہ یا غلط استعمال کہلاتا ہے۔
- سافٹ ویئر بنانے والے کے ساتھ کیے گئے معاہدہ (Agreement) کو وارنٹی یا ذمہ داری کہا جاتا ہے۔
- پیٹنٹ ایک آئیڈیا کی حفاظت کرتا ہے تاکہ اس کا غلط استعمال نہ ہو اور مالک اس کے مکمل حقوق رکھے گا۔
- قدر (Value) اور افادیت (Usefulness) کی حفاظت کے لیے ہم تجارتی راز محفوظ رکھتے ہیں۔
- کمپیوٹر سے دور دراز بیٹھ کر حملہ کیا جا سکتا ہے اس طرح حساس معلومات سبوتاژ ہو جاتی ہیں۔
- کرپٹوگرافی یا خفیہ کاری کا مطلب ہے کہ ڈیٹا کو نہ پڑھی جانے والی صورت میں تبدیل کرنا جسے سائفر ٹیکسٹ (Ciphertext) کہتے ہیں۔ اس کو پڑھنے کے لیے ایک کلید یا کی (Key) کی ضرورت ہوتی ہے۔
- پاس ورڈ کو ایک سسٹم میں داخل ہونے کے لیے تصدیق کے طور پر استعمال کیا جاتا ہے۔
- ایسا جرم جس میں کمپیوٹر نیٹ ورک یا آلات کیے جاتے ہیں سائبر کرائم کہلاتا ہے۔
- غیر قانونی طور پر کسی دوسرے کے کمپیوٹر تک رسائی حاصل کرنا ہیکنگ (Hacking) کہلاتا ہے۔
- DOS اٹیک ایک ایسا سائبر حملہ ہے جس میں ایک مشین یا نیٹ ورک وسائل کو صارفین کے لیے بیکار بنانے کے لیے استعمال کیا جاتا ہے۔

EXERCISE

4.1 صحیح جواب کی نشاندہی کریں۔

1- درجہ ذیل میں سے کیا سافٹ پائیریسی (Piracy) کی اقسام میں شامل ہے۔

(i) سافٹ لفٹنگ
(ii) ذمہ داری
(iii) کلائنٹ سرور اوور یوز
(iv) آن لائن پائیریسی

2- درجہ ذیل میں سے کون سا سائبر کرائم نہیں ہے۔

(i) ہیکنگ
(ii) فشنگ کرائم
(iii) شناخت کی چوری
(iv) ڈیکریپشن

3- درجہ ذیل میں سے کون سا عمل فشنگ ای میل کی خوبی نہیں ہے۔

(i) سرکاری ڈیٹا کی خلاف ورزی کی اطلاع
(ii) ای میل اکاؤنٹ اپ ڈیٹ
(iii) آئی ٹی یاددہانی
(iv) اصل ویب سائٹ کی ڈومین

4- درجہ ذیل میں سے فشنگ ویب سائٹ کی خوبی نہیں ہے۔

(i) اصل ویب سائٹ جیسی ڈومین
(ii) زائرین کو جمع کرنے کے لیے فارم کا استعمال
(iii) ویب مواد سے اصل لنک
(iv) ای میل اکاؤنٹ اپ ڈیٹس

5- درجہ ذیل میں سے کون سی اچھے پاس ورڈ کی خوبی نہیں ہے۔

(i) آٹھ حرفی طوالت
(ii) یوزر نیم (Username) پر مشتمل نہ ہو
(iii) بڑے حروف پر مشتمل ہے
(iv) پاس ورڈ صرف آپ کے نام پر مشتمل ہے

4.2 خالی جگہ پُر کریں۔

(i) سافٹ ویئر کی غیر قانونی نقول بنانا۔۔۔۔۔۔۔۔۔۔۔۔۔۔۔کہا جاتا ہے۔

(ii) ۔۔۔۔۔۔۔۔۔۔۔۔۔کسی بھی طرح کی معلومات کی پروسیسنگ کے لیے عمومی اصطلاح ہے جسے ریاضیاتی شکل میں ظاہر کیا جا سکتا ہے۔

(iii) ۔۔۔۔۔۔۔۔۔۔۔۔۔ڈیٹا کی خفیہ کاری کا عمل ہے۔

(iv) جب ایک کی (Key) کے حروف خفیہ کاری کرنے والے لفظ کے حروف سے کم ہوں تو کی لیٹرز کو دوبارہ لکھنا۔---------- کہلاتا ہے۔

(v) -----------۔ایسا سائبر اٹیک ہے جو کسی مشین یا نیٹ ورک وسائل کو صارف کے استعمال کے ناقابل بنا دیتا ہے۔

4.3 ان سوالوں کا جواب دیں۔

(i) سائیفر ٹیکسٹ (Cyphertext) کی وضاحت کریں؟

(ii) ہمیں ایک انسٹالیشن کی (Key) کی ضرورت کیوں ہوتی ہے جبکہ ایک سافٹ ویئر کو پاس ورڈ کے ساتھ محفوظ کیا جاسکتا ہے؟

(iii) DOS اٹیک کی وضاحت کریں۔

(iv) کیپچا (Captcha) کو ویب سائٹ پر دینے کی کیا وجہ ہے؟

(v) پیٹنٹ (Patent) کیا ہے اور ہمیں اسے رجسٹر کرنے کی ضرورت کیوں ہے؟

سرگرمی: 4.8

ٹیچر کلاس کو گروپوں میں تقسیم کرے گا اور ہر گروپ میں زیادہ سے زیادہ چار طالب علم ہوں۔ طالب علم پانچ حروف سے کی (Key) بنائیں گے اور اس کی (Key) کو استعمال کرتے ہوئے چار خطوط کا سائیفر ٹیکسٹ بنائیں گے۔ ہر خفیہ پیغام میں زیادہ سے زیادہ دس حروف موجود ہوں۔ ٹیچر ان پیپرز کو طالب علموں سے اکٹھا کرے گا اور ان کو بے ترتیب انداز میں مختلف گروپوں میں تقسیم کرے گا اور انہیں ڈیکرپٹ (Decrypt) کرنے کا کہا جائے گا۔ جو گروپ سب سے پہلے ٹیکسٹ کو ڈیکرپٹ کرے گا وہ فاتح قرار پائے گا۔