17
பாடம்

5WD6QT

மின்–வணிக பாதுகாப்பு அமைப்புகள்

கற்றலின் நோக்கங்கள்

- மின்–வணிக பாதுகாப்பு அமைப்புகளின் அடிப்படைகளைத் தெரிந்து கொள்ளுதல்
- பல்வேறு வகையான மின்–வணிக அச்சுறுத்தல்களை புரிந்து கொள்ளுதல்
- மின்–வணிக பாதுகாப்பின் பரிமாணங்கள் பற்றி அறிந்து கொள்ளுதல்
- மின்–வணிக பரிமாற்றத்தில் பாதுகாப்பு தொழில்நுட்பங்கள் பற்றி அறிந்து கொள்ளுதல்

அறிமுகம்

இணையத்தின் வேகமான வளர்ச்சியுடன், இணையதள பரிவர்த்தனைகள் முக்கிய வர்த்தக மாதிரியாக மாறிவிட்டன. இணைய வளங்களை அடிப்படையாக கொண்ட மின்–வணிக பரிவர்த்தனைகளை பொதுமக்கள் ஏற்றுக் கொள்ளத் தொடங்கியுள்ளனர். இணைய பரிவர்த்தனைகளால் ஏற்படும் வசதியைப் பயன்படுத்தும் போது, பரிமாற்றங்களின் பாதுகாப்பு மிகவும் கவனத்தை ஈர்த்துள்ளது. இணையத்தின் உள்ளார்ந்த வெளிப்படை தன்மை (Openness) மற்றும் வளப்பகிர்வு மின் பரிவர்த்தனையின் பாதுகாப்பைக் கடுமையாக அச்சுறுத்துகிறது. மின் வணிக பாதுகாப்பு அச்சுறுத்தல்கள் வருவாய் இழப்பு மட்டுமல்லாது நிறுவனங்களின் நற்பெயரையும் பாதிக்கும்.

17.1 மின்–வணிக பாதுகாப்பு அமைப்புகள்

எந்த ஒரு வளர்ந்துவரும் மின் வணிகத்திற்கும் பாதுகாப்பு முக்கியக் காரணியாக உள்ளது. வணிக பரிமாற்ற நடவடிக்கைகளில் உள்ள பாதுகாப்பு அச்சுறுத்தல்களைத் தீர்த்தல் என்பது மின்–வணிகத்தின் சீரான வளர்ச்சியை உறுதிப்படுத்துவதற்கான அடிப்படையாகும்.

> மின்–வணிக பாதுகாப்பு என்பது இணையம் மூலம் மின்–வணிக பரிவர்த்தனைகளைப் பாதுகாப்பாக வழிநடத்தும் நெறிமுறைகளைக் கொண்ட ஒரு தொகுப்பு ஆகும்.

17.2 மின்–வணிக பாதுகாப்பு அச்சுறுத்தல் வகைகள்

மின்–வணிகமானது தகவல் தொழில்நுட்பம் மற்றும் கணிப்பொறி வலையமைப்புகளின் அடிப்படையில் செயல்படுவதால், மரபுசார் வணிகங்களுடன் ஒப்பிடுகையில் அது தொடர்ச்சியான பல பாதுகாப்பு பிரச்சனைகளை எதிர்கொள்ள வேண்டியுள்ளது. மின்–வணிகப் பாதுகாப்பு

அச்சுறுத்தல்கள் தற்செயலானவையோ (மனிதத் தவறுகளால் ஏற்படுவது) அல்லது உள்நோக்கம் கொண்டவையாகவோ இருக்கலாம்.

உங்களுக்குத் தெரியுமா? நச்சுநிரல், கணினிகளுக்கு தீங்கு விளைவிக்கிறது. அதன்மூலம், மின்–வணிகத்தின் செயல்திறன் மற்றும் சீரான செயல்பாட்டில் பாதிப்பை ஏற்படுத்துகிறது. சில நச்சுநிரல்கள் கணினியில் சேமித்து வைக்கப்பட்டுள்ள அனைத்து தகவல்களையும் அழித்து, பெரிய அளவில் வருவாய் மற்றும் நேர விரயத்தை ஏற்படுத்துகின்றன. கணிப்பொறி நச்சுநிரல்களின் தோற்றமும் அவற்றின் வகைகளும் கடந்த தசாப்தத்தில் மிக வேகமாக அதிகரித்துள்ளன. நச்சுநிரல் பரவுவதற்கு சிறந்த ஊடகமாக இணையம் மாறியிருக்கிறது. பல புதிய நச்சுநிரல்கள் இணையத்தின் வழியாக நேரடியாக பரவி மின் வணிகங்களுக்கு பெரும் பொருளாதார இழப்பை ஏற்படுத்துகிறது.

வெளிநாட்டு அல்லது உள்நாட்டு, நிறுவனத்தின் உள்ளே அல்லது வெளியே, குழு அல்லது தனிநபர், வியாபார போட்டியாளர்கள் அல்லது அதிருப்தி தொழிளார்கள், தீவிரவாதிகள் அல்லது ஹேக்கர்கள், திறமை, தொழில் நுட்ப அறிவு, வாய்ப்பு மற்றும் தீங்கு விளைவிக்கும் நோக்கம் கொண்ட எவரும் மின்–வணிகத்தில் ஒரு சாத்தியமான அச்சுறுத்தலாக இருக்க முடியும். எல்லா வணிகமும் தனக்கான பிரச்சினைகளை பெற்றிருந்தாலும், மின்–வணிகம் பின்வரும் குறிப்பான அச்சுறுத்தல்களை எதிர்கொள்ள நேரிடும்.

1. **தகவல் கசிவு (Information Leakage):** மின்–வணிகத்தில் வர்த்தக ஆவண இரகசியங்கள் கசிவு இரண்டு முக்கிய பரிவுகளை கொண்டுள்ளது: (அ) விற்பனையாளர் மற்றும் வாடிக்கையாளருக்கு இடையிலான பரிமாற்றத்தின் உள்ளடக்கம் மூன்றாம் தரப்பினரால் திருடப்படுவது. (ஆ) வணிகர் அல்லது வாடிக்கையாளரால் வழங்கப்பட்ட ஆவணங்கள் மற்றவரால் சட்ட விரோதமாக பயன்படுத்தப்படுவது. இவ்வாறு மின்–ஆவணங்களை இடைமறித்து திருடுதல் தகவல் கசிவு என அழைக்கப்படுகிறது.
2. **தரவு சிதைப்பு (Tampering):** தரவுகளின் நம்பகத்தன்மை மற்றும் நேர்மை தொடர்பான பிரச்சினை மின்–வணிகத்தின் முக்கிய சிக்கலாக உள்ளது. இணையத்தின் வழியாக தரவுகளைப் பரிமாறும் போது ஹேக்கர்களால் அத்தரவுகள் பல்வேறு தொழில்நுட்பங்கள் வாயிலாக தவறானதாக மாற்றி இலக்கு கணிப்பொறிக்கு அனுப்பப்படுகிறது. இதன் மூலம் தரவுகளின் நம்பகத்தன்மை சிதைக்கப்படுகிறது.

உங்களுக்குத் தெரியுமா? ஃபிஷிங் (Phishing) என்பது ஒரு வகை மின்–வணிக அச்சுறுத்தலாகும். உண்மையான வங்கி அதிகாரியாக தன்னை பாசாங்கு செய்யும் ஒருவர், மின்னஞ்சல், தொலைபேசி அல்லது குறுஞ்செய்தி மூலம் பயனரை தொடர்பு கொண்டு அவர்களின் வங்கி கணக்கு எண், கடன் அட்டை விவரங்கள், OTP, PIN அல்லது கடவுச்சொற்கள் போன்ற முக்கிய தரவை கேட்டு தனிநபர்களை வலையில் சிக்க வைக்க முயற்சிப்பார். அதன் விளைவு அடையாள திருட்டு மற்றும் நிதி இழப்பு போன்ற பேரழிவு செயல்களுக்கு வழிவகுக்கும்.

XII CompApp_Tamil version CHAPTER 17.indd 262 21-04-2020 12:29:30

3. **பண மோசடிகள் (Payment frauds):** பணம் மோசடிகள் நட்பான மோசடி– Friendly Fraud (வாடிக்கையாளர் பொய்யான தகவல் தந்து, பணம் திரும்ப கொடுக்க கோருதல்), தெளிவான மோசடி – Clean Fraud (திருடப்பட்ட ஒரு கடன் அட்டையை பயன்படுத்தப்படுத்தி பொருட்களை வாங்குதல்) முக்கோண மோசடி – Triangulation Fraud (போலி நிகழ்நிலை கடைகள் மலிவு விலை சலுகைகள் அறிவித்து கடன் அட்டை தகவல்களை சேகரித்தல் அத்தகவல்களை விற்றல்) முதலிய உப தொகுப்புகளைக் கொண்டுள்ளன.

4. **தீங்கிழைக்கும் நிரல் அச்சுறுத்தல்கள் (Malicious code threats):** ஒரு ஹேக்கருக்கு மின்–வணிக தளத்தில் பணம்மற்றும்பயனர்பற்றியதகவல்களை ஊடுருவி பெற பல பலவீனமான பகுதிகள் உள்ளன. தீங்கிழைக்கும் நிரல்கள், Cross Site Scripting, அல்லது SQL Injection மூலம், ஒரு ஹேக்கர் கடன் அட்டை தகவலை பிரித்தெடுத்து, அதனை கள்ளச் சந்தைகளில் (Black Market) விற்பனை செய்வார். பின் அத்தகவல்களை பயன்படுத்தி மின்–வணிகப் பரிவர்த்தனைகள் அல்லது ஏடிஎம் ல் பணம் எடுத்தல் போன்றவற்றின் மூலம் பெரும் நஷ்டம் உண்டாக்கும் மோசடி நடைபெறுது.

5. **பரவல் சேவை மறுக்கப்படல் தாக்குதல்கள் (Distributed Denial of Service – DDoS):** இது ஒரு மின்–வணிகத் தளத்தின் சேவையகத்திற்கு மிக அதிக வேண்டுகோள்களை தொடர்ந்து அனுப்புவதன் மூலம் அதனை முடக்கும் செயல் ஆகும். Botnet யை பயன்படுத்தி பல அடையாளம் தெரியாத கணிப்பொறிகளில் இருந்து இந்த தாக்குதல் நடத்தப்படும். இந்தத் தாக்குதல் சேவையகத்தின் திறனை குறைத்து அதனை செயலிலக்கச் செய்யும். DDoS தாக்குதல் Network Flooding என்றும் அழைக்கப்படுகிறது.

6. **சைபர் squatting (Cyber Squatting):** இது பின்னர் அதிக இலாபத்திற்கு விற்க வேண்டும் என்ற நோக்கத்தில் மற்றொரு நபர் விரும்பக்கூடிய ஒரு இணைய களப்பெயரைப் (Domain Names) பதிவு செய்யும் சட்டவிரோத நடைமுறையாகும். இது புகழ்பெற்ற வர்த்தக முத்திரைகள் மற்றும் வணிகப் பெயர்களை குறிப்பிட்ட நிறுவனம் தங்களது களப்பெயர்களாக பதிவுசெய்வதற்குமுன்பதிவுசெய்வதாகும். மேலும் சைபர் squatting என்பது ஒரு புகழ் பெற்ற / நற்பெயர் பெற்ற நிறுவனத்தின் பெயரில் போலி வலைப்பக்கத்தை உருவாக்கி நிறுவனத்தின் அதிகாரபூர்வ வலைப் பக்கம் என நம்பச் செய்து வாடிக்கையாளரைத் ஏமாற்றும் செயல் ஆகும்.

உங்களுக்குத் தெரியுமா?

செப்டம்பர் 2015 ல், "google.com" என்ற களப்பெயரை கூகிளின் முன்னாள் ஊழியர் 12 அமெரிக்க டாலர்களுக்கு வாங்கி, பின்னர் அதை கூகிள் நிறுவனத்திற்கே 6006.13 அமெரிக்க டாலர்களுக்கு விற்பனை செய்தார்.

7. **டைபோபைரஸி / தட்டச்சுப்போலி (Typopiracy):** டைபோபைரஸி என்பது சைபர் squattingன் ஒரு வகையாகும். சில போலி வலைத்தளங்கள் பயனர்களின் பொதுவான தட்டச்சு பிழைகளை பயன்படுத்தி அவர்களை தங்கள் வலைத்தளத்திற்கு திசை திருப்பும் மோசடி ஆகும். இவர்கள் தங்களது இணையதளங்களுக்கு தற்செயலான போக்குவரத்தை உருவாக்க ஏதுவாக சில பிரபலமான களப்பெயர் போன்றே தங்கள் வலைத்தளத்திற்கு பெயரிடுகின்றனர். எ.கா: www.goggle.com, www.faceblook.com

XII CompApp_Tamil version CHAPTER 17.indd 263 21-04-2020 12:29:30

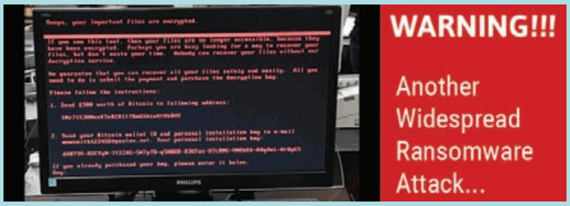
உங்களுக்குத் தெரியுமா? ஹேக்கிங் என்பது கணிப்பொறி அல்லது வலையமைப்பிற்குள் அங்கீகரிக்கப்படாத ஊடுருவலை குறிக்கிறது. அதாவது சட்டவிரோதமாக கணிப்பொறியின் பாதுகாப்பு அரணை உடைத்து, இணையத்தளத்தில் உள்புகுதல் மற்றும் இரகசிய தகவலை இடைமறித்தல் செயல் ஆகும். ஹேக்கர்கள் தங்கள் போட்டியாளர்களுக்கு தீங்கிழைக்க இதை போன்ற தகவல்களை தங்களுக்கு சாதகமாக மாற்றவோ, தவறாகப் பயன்படுத்தவோ அல்லது அழிக்கவோ செய்வார்கள்.

17.3 மின்–வணிக பாதுகாப்பின் பரிமாணங்கள்

பாதுகாப்பு சிக்கல்கள் மின்–வணிகத்திற்கு மிகவும் கவலையளிக்கும் பிரச்னையாக இருப்பதால், மின்–வணிக செயல்பாடுகளின் பாதுகாப்பை உறுதி செய்வது மின்–வர்த்தகத்தின் முக்கிய ஆராய்ச்சித் துறையாக மாறிவிட்டது. மின்–வணிகம் தொடர்புடைய சில பாதுகாப்பு அம்சங்கள் பின்வருமாறு.

- அங்கிகாரம் (Authenticity): தரவு மூலத்தை அங்கிகரித்தல் மற்றும் பங்கேற்பாளர்களின் அடையாளத்தை சரிபார்த்தல்.
- இருப்பு (Availability): தரவு தாமதம் அல்லது நீக்கத்தை தடுத்தல். அதன் மூலம் ஒரு மின் வணிக தளம் தொடர்ந்து செயல்படுவதை உறுதிப்படுத்துதல்.
- முழுமை (Completeness): அனைத்து வர்த்தகத் தகவல்களையும் ஒன்றிணைத்தல்.
- இரகசியத்தன்மை (Confidentiality): அங்கீகரிக்கப்படாத நபர்களிடமிருந்து தரவை பாதுகாத்தல் அல்லது அங்கீகரிக்கப்பட்ட பயனர்களுக்கு மட்டுமே தரவு கிடைக்கும் என்பதை உறுதிப்படுத்துதல்.
- திறனுடைமை (Effectiveness): வன்பொருள், மென்பொருள் மற்றும் தரவை முழுமையாகவும் திறம்படவும் கையாளுதல்.
- நேர்மை (Integrity): அங்கீகரிக்கப்படாத தரவு மாற்றத்தை தடுத்தல். தரவு மாற்றமடையாமல் அல்லது மாற்றியமைக்கப்படாமல் இருத்தல்.
- மறுதலிக்கப்படாதிருத்தல் (Non–repudiation): உடன்படிக்கை மீறாதிருத்தல்.
- தனியுரிமை (Privacy): வாடிக்கையாளர்களின் தனிப்பட்ட தரவுகளை பிறர் பயன்படுத்தாமல் தடுத்தல். தரவுக் கட்டுப்பாட்டை வழங்குதல்
- நம்பகத்தன்மை (Reliability): தனிநபர்கள் அல்லது நிறுவனங்களின் நம்பகத்தன்மையை அடையாளங்காணல்.
- மீளாய்வு திறன் (Review ability): தணிக்கை நடவடிக்கைகள் மற்றும் வணிகச் செயல்பாடுகளை கண்காணிக்கும் திறன்.

உங்களுக்குத் தெரியுமா? பணையத் தீநிரல் (Ransomware) என்பது இலக்கு கணிப்பொறியின் அனைத்து கோப்புகளையும் குறியாக்கம் செய்து பணம் செலுத்தப்பட்டாலன்றி அதிமுக்கிய தரவை வெளியிடுவதாக அச்சுறுத்தும் ஒரு வகை தீநிரல் ஆகும்.



XII CompApp_Tamil version CHAPTER 17.indd 264 21-04-2020 12:29:30

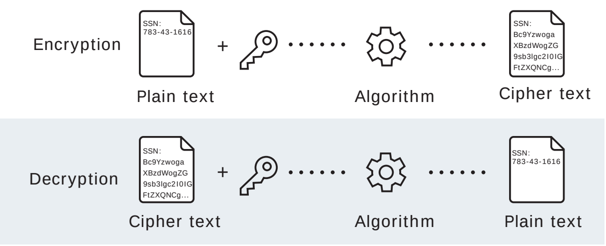
17.4 மின்–வணிக பரிமாற்றத்தின் பாதுகாப்பு தொழில்நுட்பங்கள்

அதிக அளவிலான ரகசியத் தகவல்கள், மின்–வணிகம் செயல்பாடுகளில் பயன்படுத்தப்படுகின்றன என்பதால், அது பாதுகாப்பான மற்றும் பாதுகாக்கப்பட்ட வலையமைபின் மூலம் பகிரப்பட வேண்டும். மின்–வணிக பரிவர்த்தனைகளில் பாதுகாப்பை உறுதிப்படுத்த அதிநவீன பாதுகாப்பு தொழில்நுட்பங்கள் தேவைப்படுகின்றன. தற்சமயம் மின்–வணிக பரிவர்த்தனையில் உள்ள பாதுகாப்பு தொழில்நுட்பங்கள் பின்வருமாறு வகைப்படுத்தப்பட்டுள்ளன

- குறியாக்கத் தொழில்நுட்பம் (Encryption technology)
- அங்கீகார தொழில்நுட்பம் (Authentication technology)
- பாதுகாப்பு அங்கீகார நெறிமுறைகள் (Authentication protocols)

17.4.1 குறியாக்கத் தொழில்நுட்பம்

குறியாக்கத் தொழில்நுட்பம் என்பது ஒரு செயல்திறன் மிக்க தகவல் பாதுகாப்பு அமைப்பாகும். குறியாக்க வழிமுறைகளைப் பயன்படுத்தி ஒரு மூல உரையைஅர்த்தமற்ற மறைஎழுத்து உரையாக மாற்றுவது குறியாக்கம் என்று வரையறுக்கப்படுகிறது. இதனால் தரவுகளின் இரகசியத்தன்மை உறுதி செய்யப்படுகிறது. குறியாக்கம் மற்றும் மறைகுறியாக்கம் வழிமுறைகள் தரவை குறியாக்கம் அல்லது



படம் 17.1 டேட்டா என்கிரிப்ஷன் மற்றும் டிக்ரிப்ஷன் செயல்முறை

குறிநீக்கம் செய்ய குறியீட்டை (key) உபயோகபடுத்துகிறது. தற்போது, இரண்டு குறியாக்க தொழில்நுட்பங்கள் பரவலாகப் பயன்படுத்தப்படுகின்றன. அவை சமச்சீர் குறியீடு குறியாக்கம் மற்றும் சமச்சீரற்ற குறியீடு குறியாக்கம்.

சமச்சீர் குறியீடு குறியாக்கம்

தரவு குறியாக்க தர நிலை (Data Encryption Standard – DES) ஒரு சமச்சீர் குறியீடு குறியாக்க நெறிமுறை ஆகும். இது அமெரிக்காவில் 1976–ல் ஃபெடரல் இன்ஃபர்மேசன் பராசசிங் ஸ்டாண்டர்ட் (Federal Information Processing Standard) அறிமுகப்படுத்தப்பட்டது.

சமச்சீர் குறியீடு குறியாக்கம் நெறிமுறை குறியாக்கம் மற்றும் மறைக் குறியாக்கம் ஆகிய இரண்டிற்கும் ஒரே குறியீட்டை பயன்படுத்துகின்றன. இதில் ஒரு குறிப்பிட்ட நீளமுடைய இயல் உரையை (Plain text), பல சிக்கலான செயல்பாடுகள் மூலம் அதே நீளம் கொண்ட மறைகுறி (Cipher text) உரையாக மாற்றப்படுகிறது.

சமச்சீர் குறியீடு குறியாக்கம் வழிமுறைகள் ஒரு குறியீட்டை மட்டுமே பயன்படுத்துவதால், கோட்பாட்டின்படி, குறியாக்கம் செய்வதற்கு பயன்படுத்தப்பட்ட துல்லியமான குறியீட்டை அறிந்தவர்கள் மட்டுமே மறைகுறியாக்கம் செய்ய முடியும். ஆனால் நெறிமுறையில் 56 பிட்டுகள் பயன்படுத்தப்படுகின்றன. DES–ல் 64 பிட்டுகள் பயன்படுத்தப்படுகிறது. இதில் 8 பிட்டுகள் சமநிலை சரிபார்க்க பயன்படுத்தப்பட்டு பின்னர் நிராகரிக்கப்படுகிறது. ஒப்பீட்டளவில் DES பல பயன்பாடுகளுக்கு பாதுகாப்பாக இல்லை.

சமச்சீரற்ற குறியீடு குறியாக்கம்

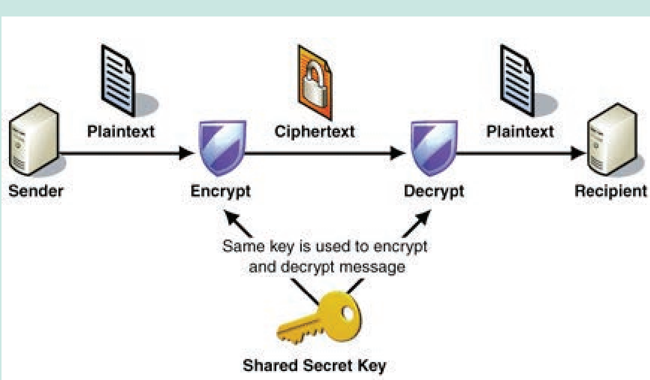
சமச்சீரற்ற குறியீடு குறியாக்கம் (Asymmetric Key Encryption) பொது குறியீடு குறியாக்கம் என்றும் அழைக்கப்படுகிறது. இது

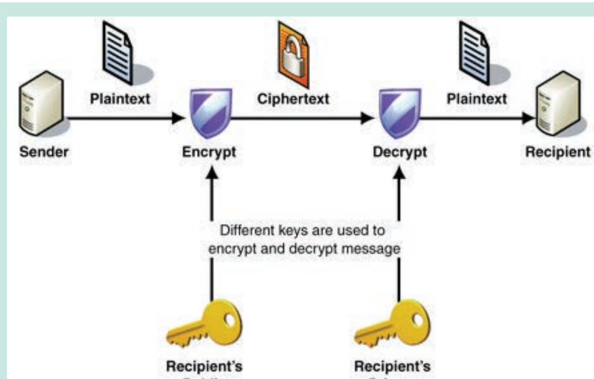
XII CompApp_Tamil version CHAPTER 17.indd 265 21-04-2020 12:29:31

பொது குறியீடு மற்றும் எண்முறைக் சான்றிதழ்களை பயன்படுத்துகிறது. 1970 ஆம் ஆண்டுவரை சமச்சீர் குறியாக்கம் முறை மட்டுமே பயன்பாட்டில் இருந்தது. இதில் அனுப்புநர் மற்றும் பெறுநர் இருவரும் ஒரே குறியீட்டை பெற்றிருக்க வேண்டும். இது குறியீடு பரிமாற்றம் மற்றும் குறியீடு மேலாண்மையில் பிரச்சனையாக இருந்தது.

சமச்சீர் குறியாக்கம் போலில்லாமல், சீரற்ற குறியாக்கத்தில் தகவல் பரிமாற்றம் செய்யும் நபர்களுக்கு மற்றவரின் தனிப்பட்ட குறியீடு தெரிந்திருக்க வேண்டியதில்லை. ஒவ்வொரு பயனரும் தனிப்பட்ட குறியீடு மற்றும் பொது குறியீடு என அவர்களின் சொந்த குறியீட்டு ஜோடியை உருவாக்குவர். பொது குறியீட்டு குறியாக்கம் முறையில் ஒரு பொது குறியீட்டை கொண்டு இயல் உரையை மறை உரையாக மாற்றி பின் ஒரு தனிப்பட்ட குறியீட்டை கொண்டு மறை உரையை மீண்டும் இயல் உரையாக மாற்றப்படுகிறது. RSA, DSS போன்றவை சமச்சீரற்ற குறியீடு குறியாக்கம் நெறிமுறைகளைப் பயன்படுத்தும் நன்கு அறியப்பட்ட குறியாக்க தொழில்நுட்பங்கள் ஆகும்.

சமச்சீர் குறியீடு குறியாக்கம்	சமச்சீரற்ற குறியீடு குறியாக்கம்
மறைகுறியாக்கம் மற்றும் குறியாக்க இரண்டிற்கும் ஒரே குறியீட்டை பயன்படுத்தப்படுகிறது.	மறைகுறியாக்கம் மற்றும் குறியாக்க இரண்டிற்கும் வெவ்வேறு குறியீடுகளை பயன்படுத்தப்படுகிறது.
மறைகுறியாக்கம் அல்லது குறியாக்கத்தின் வேகம் மிக அதிகம்.	மறைகுறியாக்கம் அல்லது குறியாக்கத்தின் வேகம் குறைவு.
தெளி உரை மற்றும் மறைக்குறியீட்டு உரை இரண்டும் ஒரே அளவானதாக இருக்கும்	தெளி உரை மற்றும் மறைக்குறியீட்டு உரையின் அளவு வெவ்வேறானதாக இருக்கும்
DES, AES, RC4 போன்ற நெறிமுறைகள் சமச்சீர் குறியீடு குறியாக்க தொழிநுட்டபத்தை பயன்படுத்துகின்றன.	RSA, ECC, DSA போன்ற நெறிமுறைகள் சமச்சீரற்ற குறியீடு குறியாக்க தொழிநுட்டபத்தை பயன்படுத்துகின்றன.
இது தரவுகளுக்கு இரகசியத்தன்மையை வழங்குகிறது.	இது இரகசியத்தன்மை, அங்கிகாரம் மற்றும் மறுதலிக்கப்படாதிருத்தல் போன்ற நன்மைகளை வழங்குகிறது.
பயனரின் எண்ணிக்கையை பொருத்து பயன்படுத்தப்படும் குறியீடுகளின் எண்ணிக்கை அடுக்குகளில் அதிகரிக்கிறது	பயனரின் எண்ணிக்கையை பொருத்து பயன்படுத்தப்படும் குறியீடுகளின் எண்ணிக்கை நேர்கோட்டில் அதிகரிக்கிறது

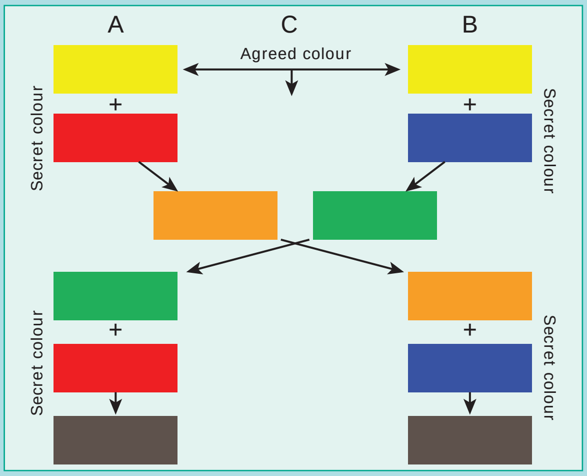




XII CompApp_Tamil version CHAPTER 17.indd 266 21-04-2020 12:29:31

உங்களுக்குத் தெரியுமா?

1976 ல் விட்ஃபீல்ட் டிஃபி மற்றும் மார்ட்டின் e ஹெல்மேன், பொது குறியீட்டு குறியாக்கம் என்ற வழிமுறையை உருவாக்கினார்கள். வண்ண விளையாட்டை பயன்படுத்தி இந்த வழிமுறையை புரிந்து கொள்ளலாம். இது C க்கு தெரியாமல் A மற்றும் B எப்படி தங்களின் ரகசியக் குறியீட்டை பெற முடியும் என்பதை விளக்குகிறது. இந்த யுக்தி இரண்டு நிகழ்வுகளை (Facts) அடிப்படையாக கொண்டது



- இரண்டு வண்ணங்களை கலந்து மூன்றாம் வண்ணத்தை பெறுவது எளிது.
- ஒரு வண்ணக் கலவையை கொடுத்து பின் சென்று அதன் சரியான மூல வண்ணங்களை கண்டுபிடிப்பது கடினம்.

1. முதலில் A மற்றும் B ஒரு பொதுவான தொடக்க வண்ணத்தை (மஞ்சள்) வெளிப்படையாக ஏற்கிறார்கள்.
2. இப்போது A ஒரு தன்னிச்சை நிறத்தைத் (சிவப்பு) தேர்ந்தெடுத்து மஞ்சளுடன் கலந்து புதிய நிறத்தை (மஞ்சள் + சிவப்பு = ஆரஞ்சு) B க்கு அனுப்புகிறார்.
3. இதேபோல் B ஒரு தன்னிச்சை நிறத்தைத் (நீலம்) தேர்ந்தெடுத்து அதை மஞ்சளுடன் கலந்து புதிய நிறத்தை (மஞ்சள் + நீலம் = பச்சை) A க்கு அனுப்புகிறார்.
4. ஹேக்கர் "C" இரண்டு புதிய நிறங்களை (ஆரஞ்சு மற்றும் பச்சை) கொண்டிருக்கலாம். ஆனால் தனிப்பட்ட நிறங்களான A யின் (சிவப்போ) அல்லது B யின் (நீலமோ) அல்ல.
5. வண்ணங்களை மாற்றி கொண்ட பிறகு மீண்டும் A அவர் பெற்ற பச்சையுடன் தனது தன்னிச்சை நிறமான சிவப்பை கலந்து புதிய கலவை நிறமான கருப்பை பெறுகிறார்.
6. மேலும் B தனது சொந்த தன்னிச்சை நிறமான நீலத்துடன் அவர் பெற்ற ஆரஞ்சை கலந்து புதிய கலவை நிறமான அதே கருப்பு நிறத்தை பெறுகிறார்.
7. பகிரப்பட்ட இரண்டு வண்ணங்களையும் C பெற்றிருந்த போதும் C யால் சரியான ஈற்று வண்ணத்தை பெற இயலவில்லை. ஏனெனில், அதற்கு A அல்லது B யின் தனிப்பட்ட நிறம் (சிவப்பு அல்லது நீலம்) ஒன்று தேவைப்படுகிறது.

17.4.2 அங்கீகார தொழில்நுட்பம்

நம்பகத்தன்மை, நேர்மை மற்றும் மறுதலிக்கப்படாதிருத்தல் ஆகியவற்றை உறுதிசெய்வதுஅங்கீகாரதொழில்நுட்பத்தின் முக்கிய பணியாகும். இதனை எண்முறைச் சான்றிதழ்கள் மற்றும் எண்முறைக் கையொப்பம் மூலம் அடையலாம்.

எண்முறைச் சான்றிதழ்கள்

ஒரு எண்முறைச் சான்றிதழ் (பொது குறியீட்டு சான்றிதழ் என்று அழைக்கப்படுகிறது) என்பது ஒருவரது பொது குறியீட்டின் (Public Key) உரிமையை நிரூபிக்க பயன்படுத்தப்படும் ஒரு மின்னணு ஆவணம் ஆகும். இந்த சான்றிதழில் அனுப்புநரின் அடையாளம் பற்றிய தகவல்கள், அனுப்புநரின் எண்முறைக் கையொப்பம் மற்றும் அவரின் பொது குறியீடு போன்ற தகவல்கள் அடங்கியிருக்கும்.

கடவுச்சீட்டு மற்றும் ஓட்டுனர் உரிமம் போன்ற அடையாள அட்டைகளின் பயன்பாடு போன்றே எண்முறை சான்றிதழின் பயன்பாடும் உள்ளது. எண்முறை சான்றிதழ் அங்கீகரிக்கப்பட்ட சான்றளிப்பு அதிகாரிகளால் (Certification Authorities – CA)

XII CompApp_Tamil version CHAPTER 17.indd 267 21-04-2020 12:29:31

> **உங்களுக்குத் தெரியுமா?** எண்முறைச் சான்றிதழ், உரிமம் பெற்ற சான்றளிக்கும் அதிகாரியால் (CA) வழங்கப்படுகிறது. NIC, Safescript, TCS, MTNL, e–Mudhra ஆகியவை இந்திய அரசால் அங்கீகரிக்கப்பட்ட சான்றளிக்கும் நிறுவனங்கள் ஆகும்.

வழங்கப்படுகின்றது. ஒருவர் எண்முறை சான்றிதழைக் கோருகையில் சான்றளிப்பு அதிகாரி விண்ணப்பதாரின் அடையாளத்தை சரிபார்ப்பார். மேலும் விண்ணப்பதாரர் அனைத்து தேவைகளையும் பூர்த்திசெய்தால் மட்டுமே, சான்றளிப்பு அலுவலர் அவரின் எண்முறை சான்றிதழை வழங்குவார். ஒரு மின்னணு ஆவணத்தில் கையொப்பமிட அனுப்புநர் எண்முறை சான்றிதழை பயன்படுத்துகையில், பெறுநர் அந்த எண்முறை கையொப்பத்தை நம்ப முடியும், ஏனெனில் அவர் சான்றளிப்பு அதிகாரியானவர் CA அனுப்புநரின் அடையாளத்தை சரிபார்த்திருப்பார் என்று நம்புகிறார்.

படம் 17.2 **எண்முறைச் சான்றிதழ்**

- Pretty Good Privacy (PGP) மற்றும் X.509 ஆகியவை புகழ்பெற்ற எண்முறைச் சான்றிதழ் வகைகள் ஆகும்.

எண்முறைக் கையொப்பம்

எண்முறைக் கையொப்பம் என்பது ஒரு குறிப்பிட்ட மின்னணு ஆவணம், செய்தி அல்லது பரிவர்த்தனை நம்பகமானதா என சரிபார்க்கப் பயன்படும் ஒரு அமைப்பு ஆகும்.

இது ஒரு பெறுநருக்கு தகவல் குறிப்பிட்ட அனுப்புநரால் தான் உருவாக்கப்பட்டது என்பதற்கான உத்தரவாதம் அளிக்கிறது. மேலும் இந்த தகவல், கையொப்பம் இடுபவரிடம்தான் தோன்றியதாகவும், நடுவில் உள்ள ஒரு cracker மூலம் மாற்றம் செய்யப்படவில்லை என்பதையும் உறுதிப்படுத்துகிறது.

எண்முறை கையொப்பங்கள், மின்னணு ஆவணங்களின் தோற்றம், தனித்துவம், நிலை மற்றும் அனுப்புநரின் ஒப்புதல் போன்றவற்றின் ஆதாரப்பூர்வமான உறுதிமொழிகளை வழங்குகிறது.

எண்முறை கையொப்பங்கள், அதிக அளவு பாதுகாப்பு மற்றும் உலக அளவிலான ஏற்பு ஆகியவற்றை வழங்குவதற்காக, பொதுக் குறியீடு உள்கட்டமைப்பை (PKI) என அழைக்கப்படும் ஒரு உலகளாவிய ஏற்றுக்கொள்ளப்பட்ட தரநிலையை பயன்படுத்துகின்றன. பல நாடுகளில், எண்முறை கையொப்பம் ஆனது பாரம்பரிய வடிவங்களான கையெழுத்திடப்பட்ட ஆவணங்களின் அதே சட்ட முக்கியத்துவத்தைக் பெற்றுள்ளது. நிதி ஆவணங்கள் அல்லது கடன் அட்டை தரவுகள் போன்ற முக்கிய ஆவணங்களில் மோசடி அல்லது தகவல் சிதைப்பை தவிர்ப்பதற்காக எண்முறை கையொப்பங்கள் பரவலாகப் பயன்படுத்தப்படுகின்றன.

XII CompApp_Tamil version CHAPTER 17.indd 268 21-04-2020 12:29:31

எண்முறைக் கையொப்பம்	எண்முறைச் சான்றிதழ்கள்
ஒரு எண்முறைக் கையொப்பம் ஒரு மின்னணு ஆவணம். செய்தி அல்லது பரிவர்த்தனை உண்மையானதா என்பதை சரிபார்க்கப் பயன்படும் ஒரு செயல்முறையாகும்.	ஒரு எண்முறைச் சான்றிதழ் என்பது சான்றிதழ் வைத்திருப்பவருக்கும் ஒரு குறிப்பிட்ட பொது குறியீட்டுக்கும் இடையில் உள்ள உறவை அதிகாரப்பூர்வமாக அங்கீகரிக்கும் ஒரு கணிப்பொறி கோப்பு ஆகும்.
அனுப்பப்படும் தரவு நம்பகத்தன்மையை சரிபார்க்க எண்முறைக் கையொப்பங்கள் பயன்படுத்தப்படுகின்றன.	அனுப்புனரின் நம்பகத்தன்மை சரிபார்க்க எண்முறைச் சான்றிதழ்கள் பயன்படுத்தப்படுகின்றன.
எண்முறைக் கையொப்பம் தரவரிசையில் இருந்தே ஒரு தரவு பாதுகாப்பாக இருப்பதை உறுதி செய்வது மற்றும் மூன்றாம் தரப்பினரால் மாற்றப்படவில்லை.	எண்முறைச் சான்றிதழ் ஒரு பொருளுடன் ஒரு எண்முறைக் கையொப்பத்தை பிணைக்கிறது
இது பரிமாறப்படும் தரவுகளுக்கு அங்கீகாரம், மறுதலிக்கப்படாதிருத்தல் மற்றும் நேர்மை ஆகியவற்றை இது வழங்குகிறது.	இது பரிமாறப்படும் தரவுகளுக்கு அங்கீகாரம் மற்றும் பாதுகாப்பை வழங்குகிறது.
எண்முறைக் கையொப்பம் Digital Signature Standard – DSS என்ற நெறிமுறையை ஐ பயன்படுத்தி உருவாக்கப்படுகிறது. இது தகவலை மறைகுறியாக்க மற்றும் குறியாக்க செய்ய SHA–1 அல்லது SHA–2 வழிமுறையைப் பயன்படுத்துகிறது.	ஒரு எண்முறைச் சான்றிதழ் Public Key Cryptography Standards (PKCS) நெறிமுறையின் அடிப்படையில் வேலை செய்கிறது. இது X.509 அல்லது PGP வடிவத்தில் சான்றிதழை உருவாக்குகிறது.
ஆவணம் அனுப்பும் முடிவில் குறியாக்கம் செய்யப்பட்டு சமச்சீரற்ற விசையைப் பயன்படுத்தி பெறும் முடிவில் குறியாக்கம் செய்யப்படுகிறது.	ஒரு எண்முறைச் சான்றிதழ் சான்றிதழ் உரிமையாளர் பெயர் மற்றும் பொது குறியீடு, காலாவதி தேதி, சான்றிதழ் ஆணையத்தின் பெயர், ஒரு சான்றிதழ் ஆணையத்தின் எண்முறைக் கையொப்பம் கொண்டிருக்கும்.

உங்களுக்குத் தெரியுமா?

பாதுகாப்பு அடையாளம் என்பது பயனர்களை அடையாளம் கண்டு அங்கீகரிக்க பயன்படும் வன்பொருள் கூறு.

17.4.3 பாதுகாப்பு அங்கீகார நெறிமுறைகள்

தற்போது மின்–வணிகத்தில் பாதுகாப்பான மின்னணு பரிவர்த்தனை மற்றும் பாதுகாப்பான சாக்கெட் அடுக்கு ஆகிய இரண்டு வகையான பாதுகாப்பு அங்கீகார நெறிமுறைகள் பரவலாகப் பயன்படுத்தப்படுகின்றன.

பாதுகாப்பான மின்னணு பரிவர்த்தனை

பாதுகாப்பான மின்னணு பரிவர்த்தனை (Secure Electronic Transaction – SET) என்பது, குறிப்பாக இணையம் வழியாக கடன் அட்டை மூலம் மின்னணு பணம் செலுத்தல்களுக்கான பாதுகாப்பு நெறிமுறை

XII CompApp_Tamil version CHAPTER 17.indd 269 21-04-2020 12:29:31

ஆகும். இது GTE, IBM, மைக்ரோசாப்ட் மற்றும் நெட்ஸ்கேப்பின் பங்களிப்புடன், 1996 ல் விசா மற்றும் மாஸ்டர்கார்டு நிறுவனங்களால் உருவாக்கப்பட்டது.

SET இன் செயலாக்கம் எண்முறைக் கையொப்பம் மற்றும் பரிமாற்ற தரவின் குறியாக்கம் ஆகியவற்றின் அடிப்படையில் செயலாக்கப்படுகிறது. மேலும் தனியுரிமையை (Privacy) உறுதிப்படுத்த, இரட்டைக் கையொப்பங்களையும் பயன்படுத்துகிறது.

SET நெறிமுறை மூன்று பங்களிப்பாளர்களை உள்ளடக்கியது: வாடிக்கையாளர், விற்பவர் மற்றும் விற்பவரின் வங்கி. இந்த அமைப்புமுறைக்கு மூன்று பங்களிப்பாளர்களிலிருந்தும் சான்றிதழ்கள் தேவைப்படுகின்றன. வாடிக்கையாளரின் மற்றும் விற்பனையாளரின் சான்றிதழ்கள் அந்தந்த வங்கிகளின் மூலம் வழங்கப்படுகின்றன. அதன் பிறகுதான் வர்த்தக பரிவர்த்தனை நடைபெற முடியும். இந்த SET நெறிமுறையுடன், கடன் அட்டை எண் விற்பவருக்கு தெரியாமல் இருக்கும், எனவே விற்பவரின் கோப்புகளில் சேமிக்கப்பட முடியாது, மேலும் ஒரு ஹேக்கர் மூலம் மீட்க முடியாது.

திறந்த பிணையத்தில், கடன் அட்டைகளை பயன்படுத்தி செய்யப்படும் மின்னணு பரிவர்த்தனையின் பாதுகாப்புக்கு இந்த செட் நெறிமுறை உத்தரவாதம் அளிக்கிறது. இதில் பரிமாற்றத் தரவு மாற்றமடையாமல் இருப்பது மற்றும் பரிவர்த்தனைகளை மறுதலிக்கப்படாமல் இருப்பது ஆகியவற்றை உறுதி செய்வதது போன்ற நன்மைகள் உண்டு. எனவே, மின்னணு கடன் அட்டை பரிமாற்றத்திற்காக சர்வதேச அளவில் அங்கீகரிக்கப்பட்ட தரமாக மாறியுள்ளது.

SET முறைமை பின்வரும் முக்கிய அம்சங்களை கொண்டுள்ளது:

- பொது குறியீடு குறியாக்கம் மற்றும் தனிப்பட்ட குறியீடு குறியாக்கம் பயன்படுத்தி தரவின் இரகசியத்தன்மையை உறுதி செய்யகிறது
- தகவல்களின் உண்மைத்தன்மையை உறுதிப்படுத்த தகவல் தொகுப்பு தொழில்நுட்பத்தை பயன்படுத்துகிறது.
- பரிவர்த்தனையில் இரு தரப்பினரின் அடையாளத்தையும் உறுதிப்படுத்துவதற்கு இரட்டைப் கையொப்பம் தொழில்நுட்பத்தை பயன்படுத்துகிறது.

படம் 17.3 http மற்றும் https இடையே வேறுபாடு

XII CompApp_Tamil version CHAPTER 17.indd 270 21-04-2020 12:29:31

பாதுகாப்பான சாக்கெட்டு அடுக்குகள்

மிகவும் பொதுவான மறைகுறியீட்டியல் நெறிமுறை பாதுகாப்பான சாக்கெட் அடுக்குகள் (Secure Sockets Layers – SSL) ஆகும். SSL என்பது இணைய பரிமாற்றங்களைப் பாதுகாப்பதற்காகன ஒரு கலப்பு குறியாக்க நெறிமுறை ஆகும். மாஸ்டர்கார்டு, பாங்க் ஆப் அமெரிக்கா, MCI மற்றும் சிலிக்கான் கிராபிக்ஸ் ஆகியோருடன் இணைந்து நெட்ஸ்கேப் நிறுவனம் SSL தரநிலையை உருவாக்கியது. இது இணையத்தில் தரவு பரிமாற்றத்தின் பாதுகாப்பை உறுதிப்படுத்துவதற்கான பொது குறியீடு குறியாக்கவியல் செயல்முறையின் அடிப்படையில் அமைந்துள்ளது.

இதன் நோக்கம் ஒரு அங்கீகார நடவடிக்கைக்கு பிறகு முனையம் மற்றும் சேவையகம் இடையே ஒரு பாதுகாப்பான தகவல்தொடர்பு தடத்தை (குறியாக்கம் செய்யபட்ட) நிறுவுவது ஆகும்.

SSL அமைப்பானது கூடுதல் பாதுகாப்பு அடுக்காகச் செயல்படுகிறது, மேலும் TCP இல் பயன்பாட்டு அடுக்கு மற்றும் போக்குவரத்து அடுக்கு ஆகியவற்றுக்கு இடையில் உள்ள தரவுகளின் பாதுகாப்பை உறுதிப்படுத்துகிறது. எடுத்துக்காட்டாக, ஒரு இணைய உலாவியைப் பயன்படுத்தி SSL பாதுகாக்கப்பட்ட மின்–வணிக தளத்துடன் பயனரை இணைக்க, மின்–வணிக தளம் எந்த ஒரு கூடுதல் கையாளுதலின்றி, குறியாக்கப்பட்ட தரவை அனுப்பும். பாதுகாப்பான சாக்கெட்ஸ் அடுக்குகள் (SSL) 2001 ல் பரிமாற்ற அடுக்கு பாதுகாப்பு (Transport Layer Security TLS) என்று பெயர் மாற்றம் செய்யப்பட்டது. ஆனால், இன்னமும் அது SSL என்ற பெயரில் பிரபலமாக அறியப்படுகிறது.

இன்று, சந்தையில் உள்ள அனைத்து உலாவிகளும் SSL நெறிமுறையை ஆதரிக்கின்றன. மேலும் பெரும்பாலான பாதுகாப்பான தகவல்தொடர்புகள் இந்த நெறிமுறை மூலமே தொடர்கின்றன. SSL நெறிமுறையில் தலையிட வேண்டிய தேவை இல்லாத பயனாளருக்கு அதன் செயலாக்கம் முழுமையாக மறைக்கப்படுகிறது. பயனர் செய்ய வேண்டிய ஒரே செயல் உரலி http:// க்கு பதிலாக https:// உடன் தொடங்குதை உறுதிப்படுத்துவது மட்டுமே. "s" (secured) என்பது, பாதுகாக்கப்பட்ட என்று பொருள்படுகிறது. இது ஒரு பச்சை நிற பூட்டு குறியையும் முன்னொட்டாக கொண்டிருக்கும்.

3D பாதுகாப்பு

"3D பாதுகாப்பு என்பது இணையத்தில் ஒரு பாதுகாப்பான கட்டணம் செலுத்தும் உதவும் நெறிமுறை ஆகும். பரிமாற்ற பாதுகாப்பின் அளவை அதிகரிக்க VISA ஆல் இது உருவாக்கப்பட்டது. பின்னர் இது மாஸ்டர்கார்ட் ஆல் ஏற்றுக்கொள்ளப்பட்டது. இது வலைத்தளம் மூலம் கொள்முதல் செய்யும் போது, கட்டண அட்டை வைத்திருப்பவரின் சிறந்த அங்கீகாரத்தை வழங்குகிறது. இந்த (XML அடிப்படையிலான) நெறிமுறையின் அடிப்படைக் கருத்து, நிதி அதிகாரமளித்தல் செயல்முறையை ஒரு நிகழ்நிலை சான்றளிப்பு அமைப்புடன் இணைப்பதாகும். இந்த சான்றளிப்பு மாதிரி 3 (Domains) களங்களை உள்ளடக்கியது (எனவே 3D என்று பெயர்பெற்றது) அவை:

1. பெறுநர் களம் Acquirer Domain
2. வழங்குநர் களம் Issuer Domain
3. இயங்குதன்மை களம் Interoperability Domain

XII CompApp_Tamil version CHAPTER 17.indd 271 21-04-2020 12:29:31

CASE STUDY

பொது குறியீடு குறியாக்கத்தை பயன்படுத்தி SSL இன் இயக்கக் கொள்கையை பின்வரும் சூழலில் எளிதில் புரிந்து கொள்ள முடியும் "குமார் ஒரு மின்–வணிக தளத்தில் (abc.com) இலிருந்து கைபேசியை வாங்குகிறார்."

1. குமார் தனது கணினி உலாவியில் மூலம் abc.com வலைத்தளத்துடன் ஒரு பாதுகாப்பான இணைப்பின் மூலம் இணைகிறார்.
2. abc.com வலைத்தளம் குமாருக்கு தனது மின்னணு சான்றிதழ் மற்றும் பொது குறியீட்டை (P) அனுப்புகிறது. சான்றிதழ் வழங்கும் அதிகாரி (CA) வழங்கிய இந்த மின்னணு சான்றிதழ் abc.com யின் அடையாளத்தை நிரூபிக்கிறது.
3. குமாரின் உலாவி சான்றிதழை சோதிக்கிறது. அது (உலாவி) பின்னர் சமச்சீர் குறியாக்க நெறிமுறையை பயன்படுத்த சேவையகத்துடன் உடன்படுகிறது. பின்னர் இந்த வழிமுறைக்கு தேவையான ஒரு குறியீட்டை (அமர்வு குறியீடு K) தோராயமாக தேர்வு செய்கிறது.
4. குமாரின் உலாவி abc.com க்கு P(K) வை அனுப்புகிறது. அதன் இரகசிய குறியீடு S யை பயன்படுத்தி, abc.com சேவையகம் S(P(K)) = K கணக்கிடுகிறது. ஆக, குமாரின் உலாவி மற்றும் abc.com சேவையகம் ஆகிய இரண்டின் வசமும் ஒரே குறியீடு உள்ளன.
5. குமார் தனது கணக்கு எண் மற்றும் பிற தரவுகளை உள்ளிடுகிறார். அவை "தகவல்' என வரையறுக்கப்படும். உலாவி, குறியீடு K வை பயன்படுத்தி குறியாக்கம் செய்யப்பட்ட இந்த "தகவலை", abc.com க்கு அனுப்புகிறது, மேலும் ஹேஷ் செயற்கூறு எனப்படும் கணித செயல்பாட்டை பயன்படுத்தி "தகவல் சுருக்கம்" ஒன்றையும் என்ற அனுப்புகிறது.
6. குறியீடு K உடன் abc.com சேவையகம் "தகவலை' மறையீடு நீக்கம் செய்ய முடியும். மற்றும் இது தகவல் சுருக்கத்தையும் கணக்கிட்டு, குமாரின் உலாவி அனுப்பிய சுருக்கத்துடன் ஒப்பிடுகிறது. அவை ஒருங்கிணைந்தால், தரவு சரியாக அனுப்பப்பட்டுள்ளதாக கருதப்படுகிறது.

நினைவில் கொள்க

- ஃபிஷிங்: தகர்பர் நம்பற்குரியவர் போல் வேடமிட்டு உள்நுழைவு சான்றுகளை போன்ற முக்கியமான தரவை தொலைபேசி, எஸ்எம்எஸ், மின்னஞ்சல் அல்லது சமூக ஊடகங்கள் மூலம் அடைவது.
- சான்றளிப்பு : அனுப்புநரின் தகவல் பெரும்பாலும் ஆவணத்தில் சேர்க்கப்படுகிறது, ஆனால் அவை துல்லியமற்றதாக இருக்கலாம். ஒரு ஆவணத்தின் ஆதாரத்தை சான்றபடுத்த அங்கீகரிக்க ஒரு எண்முறை கையொப்பம் பயன்படுத்தப்படலாம்.
- நேர்மை: பல சூழ்நிலைகளில், ஆவணத்தின் அனுப்புநர் மற்றும் பெறுநருக்கு, இந்த ஆவணம் இடமாற்றத்தின் போது எந்த வகையிலும் சிதைக்கப்படவில்லை என்ற நம்பிக்கை தேவைப்படும். ஆவணம் எண்முறை கையொப்பமிடபட்டிருந்தால், பின் ஆவணத்தில் எந்தவொரு திருத்தமும் கையொப்பத்தை செல்லத்தாகாததாக்கும்.

- மறுதலிக்கப்படாதிருத்தல்: மறுதலித்தல் ஒரு செய்திக்கான பொறுப்புடைமையைக் துறக்கும் செயலை குறிக்கிறது. மறுதலிக்கப்படாதிருத்தல் ஆவணத்தில் எண்முறை கையொப்பமிட்டவர் அதை நிராகரிக்கமுடியாததை உறுதிசெய்கிறது. எண்முறை கையொப்பமிட்ட ஆவணங்கள் அதன் பெறுநருக்கு ஆதாரத்தை வலுப்படுத்துகிறது. எனவே, பின் ஒரு நேரத்தில் எளிதில் மறுக்க முடியாது என்பதால் எண்முறை கையொப்பத்தை, பெறுநர் வலுவாக வலியுறுத்த முடியும்.
- எண்முறை கையொப்பம்: எண்முறை கையொப்பம் மற்றும் எண்முறை சான்றிதழுக்கும் இடையே உள்ள வித்தியாசம் என்னவெனில், எண்முறை சான்றிதழ், ஒரு தரவுடன் ஒரு கையொப்பத்தை பிணைக்கிறது. ஆனால் எண்முறை கையொப்பம், அது அனுப்பப்பட்ட புள்ளியிலிருந்து ஒரு தகவல் பாதுகாப்பாக இருப்பதை உறுதி செய்கிறது. வேறு வார்த்தைகளில் கூறுவதானால்: அனுப்புபவரின் நம்பகத்தன்மை குறித்து சரிபார்க்க எண்முறை சான்றிதழ்கள் பயன்படுத்தப்படுகின்றன, அதே நேரத்தில் எண்முறை கையொப்பங்கள் அனுப்பப்படும் தரவின் நம்பகத்தன்மை பற்றி சரிபார்க்க பயன்படுத்தப்படுகிறது.
- சான்றளிப்பு அதிகார அமைப்பு களஞ்சியம் என்று அழைக்கப்படும் ஒரு பொது குறியீடு தரவுத்தளத்தை பராமரிக்கிறது. அதன்மூலம் எண்முறை கையொப்பங்களுடன் பயனரை சரிபார்க்க முடியும். சான்றிதழ் அதிகார அமைப்பால் காலாவதியான சான்றிதழ்கள் பொதுவாக தரவுத்தளத்தில் இருந்து நீக்கப்படும்.
- முரட்டு தாக்குதல்கள் என்பது எந்த குறியாக்கத்தையும் உடைக்க எளிய தாக்குதல் முறை ஆகும்; அதாவது சாத்தியமான எல்லா குறியீடுகளையும் ஒவ்வொன்றாக முயற்சி செய்வது.

கலைச்சொற்கள்

3D	இணைய கடன் அட்டை மற்றும் பற்று அட்டை பரிவர்த்தனைகளுக்கு வழங்கப்படும் ஒரு கூடுதல் பாதுகாப்பு அடுக்கு.
மறைஎழுத்து	குறியாக்கம் செய்யப்பட்ட தரவு. பொதுவாக குறியாக்க வழிமுறையின் வெளியீடு.
Hacker – குறும்பர்	முக்கிய தரவுக்களை அணுக, கணிப்பொறி வலையமைப்பின் பாதுகாப்புச்சுவர் உடைக்கும் ஒரு நபர்.
மறையீட்டுப் பகுப்பாய்வு	மறைக்கப்பட்ட தரவு அல்லது மறைஎழுத்து உள்ள சந்தேகத்திற்குரிய ஆவணத்தை பகுப்பாய்வு செய்தல்.
Decipher மறையீடு நீக்கம்	மறையீடு நீக்கம் செய்ய ஒரு முறையான வழிமுறை.
கள பண்புரிமைப் பெயர்	ஒரு மின்–வணிக வலைத்தள முகவரி, எடுத்துக்காட்டு www.amazon.com
குறிமறையாக்கம்	அங்கீகரிக்கப்படாத அணுகலிலிருந்து தரவுகளை பாதுகாக்க / மறைக்க ஒரு வழிமுறையை பயன்படுத்தி ஒழுங்கற்ற தரவாக மாற்றும் முறை.
நட்பான மோசடி	வாடிக்கையாளர், பொருட்களை பெறவில்லை என்ற பொய்யான தகவல் தந்து செலுத்திய பணம் திரும்ப கொடுக்க கோருதல்
Hacking / தகர்ப்பான்	ஒரு கணிப்பொறி முறைமை அல்லது வலையமைப்பில் நுழைய அங்கீகரிக்கப்படாத உட்புகுதல். அதாவது சட்ட விரோதமாக ஒரு வலைத்தளத்தை அணுக பாதுகாப்பை உடைத்தல் மற்றும் இரகசிய தகவல்களை இடைமறித்தல்.
செய்தி சுருக்கம் / தொகுப்பு	ஒரு வகை ஹேஷ் செயற்கூற்றை பயன்படுத்தி இலக்கங்களின் ஒற்றை சர வடிவத்தில் தரவை உருவகித்தல்.

One–Time Password (OTP) ஒரு (அமர்வு) நேர கடவுச்சொல்	ஒரு உள்நுழைவு அமர்வு அல்லது பரிமாற்றத்திற்கு மட்டும் செல்லுபடியாகும் கடவுச்சொல். மின்–பரிவர்த்தனைக்கான ஆற்றல் வாய்ந்த பாதுகாப்பு வழங்குகிறது.
PIN (Personal Identification Number) தனிப்பட்ட அடையாள எண்	அட்டை அடிப்படையிலான பணம் செலுத்தும் முறையில் நுகர்வோர்களுக்கு ஒதுக்கப்படும் நிலையான எண்.
Plaintext / cleartext இயல் உரை	இது குறியாக்கம் செய்யப்படாத தகவல். உள்ளீட்டுத் தரவு சில்லு என்றும் அழைக்கப்படுகிறது
Traffic	ஒரு குறிப்பிட்ட தளத்திற்கு பார்வையாளர்களின் எண்ணிக்கையை குறிக்கும் ஒரு குறியீடு.

எங்கே? ஏன்? எப்படி? விளக்குக எப்பொழுது? ஏன்? என்ன? எங்கே? எழுதுக எப்படி?

வினாக்கள்

JHTJJC

பகுதி – அ

I. சரியான விடையைத் தேர்ந்தெடுத்து எழுதுக

1. மின்–வணிகத்தில், திருடப்பட்ட கடன் அட்டை ஒன்றை பொருட்களை வாங்க பயன்படுத்தப்படும்போது, அது _______________ என அழைக்கப்படுகிறது.
   அ) நட்பு மோசடி
   ஆ) தெளிவான மோசடி
   இ) முக்கோன மோசடி
   ஈ) சைபர் SQUATTING

2. பின்வருவனவற்றுள் எது மின்–வணிக பாதுகாப்பு உறுப்பு அல்ல?
   அ) நம்பகத்தன்மை
   ஆ) ரகசியத்தன்மை
   இ) ஃபிஷிங்
   ஈ) தனியுரிமை

3. சீரற்ற குறியாக்கம் ___________ என்றும் அழைக்கப்படுகிறது.
   அ) பாதுகாப்பான மின்னணு பரிவர்த்தனை
   ஆ) சான்றளிப்பு அதிகாரசபை
   இ) பொது குறியீடு குறியாக்கம்
   ஈ) பணம் செலுத்தல் தகவல்

4. கீழ் கண்ட எவை பாதுகாப்பு அங்கீகார தொழில்நுட்பம் அல்ல
   i. எண்முறைக் கையொப்பம்
   ii. எண்முறைக் கால முத்திரை
   iii. எண்முறைக் தொழில்நுட்பம்
   iv. எண்முறைக் சான்றிதழ்கள்
   அ) a. i, ii & iv
   ஆ) iii & iv
   இ) i, ii & iii
   ஈ) மேற்கூறிய அனைத்தும்

5. PGP யின் விரிவாக்கம் ------
   அ) Pretty Good Privacy
   ஆ) Pretty Good Person
   இ) Private Good Privacy
   ஈ) Private Good Person

6. இணைய வழி கடன் அட்டை பரிவர்த்தனைகளில் கீழ்கண்ட_______ நெறிமுறை பயன்படுத்தப்படுகிறது.
   அ) பாதுகாப்பான மின்னணு பரிவர்த்தனை (SET)
   ஆ) எண்முறைக் சான்றிதழ்கள்
   இ) சமச்சீர் குறியீடு குறியாக்கம்
   ஈ) பொது குறியீடு குறியாக்கம்

XII CompApp_Tamil version CHAPTER 17.indd 274 21-04-2020 12:29:32

7 பாதுகாப்பான மின்னணு பரிவர்த்தனை (SET) __________ ஆண்டில் உருவாக்கப்பட்டது

அ) 1999 ஆ) 1996

இ) 1969 ஈ) 1997

8. பாதுகாப்பான சாக்கெட் அடுக்கு (SSL) நெறிமுறைகளைப் பயன்படுத்தும் இணையதளங்களை ______________ மூலம் அடையாளம் காணலாம்

அ) html:// ஆ) http://

இ) htmls:// ஈ) https://

9. 3-D பாதுகாப்பு நெறிமுறை ______ ஆல் உருவாக்கப்பட்டது

அ) VISA ஆ) MASTERPAY

இ) RUPAY ஈ) PAYTM

10. பின்வருவனவற்றுள் RANSOMWARE தொடர்பான சரியான கூற்று எது?

அ) தீநிரலின் ஒரு உப தொகுப்பு அல்ல

ஆ) RANSOMWARE உடனடியாக கோப்பை நீக்குகிறது.

இ) TYPOPARICY என்பது ஒரு வகையான RANSOMWARE

ஈ) பாதிக்கப்பட்டவர்களிடமிருந்து கோப்புகளை மீட்க பணம் கோரப்படும்

பகுதி – ஆ

II. மூன்று வரிகளில் விடையளிக்கவும்

1. தகவல் கசிவு பற்றி எழுதுக.
2. டைபோபைரஸி பற்றி சிறுகுறிப்பு வரைக.
3. ஃபிஷிங் (Phishing) பற்றி எழுதுக.
4. மின்-வணிகத்தின் பல்வேறு வகையான பாதுகாப்புத் தொழில்நுட்பங்களை பட்டியலிடுக
5. எண்முறைக் கையொப்பம் பற்றி எழுதுக.

பகுதி – இ

III. ஒரு பத்தியளவில் விடையளிக்கவும்

1. மின்-வணிக பாதுகாப்பு என்றால் என்ன?
2. ஏதேனும் இரண்டு மின்-வணிக பாதுகாப்பு அச்சுறுத்தல்களை பட்டியலிடுக.
3. சமச்சீரற்ற குறியீடு குறியாக்கம் பற்றி எழுதுக.
4. எண்முறைச் சான்றிதழ் பற்றி குறிப்பு வரைக.
5. 3D பாதுகாப்பு பண பரிவர்த்தனை நெறிமுறைகளை விளக்கி எழுதவும்

பகுதி – ஈ

IV. ஒரு பக்க அளவில் விடையளிக்கவும்

1. மின்-வணிக பாதுகாப்பின் பரிமாணங்கள் பற்றி எழுதுக.
2. சமச்சீர் குறியீடு குறியாக்கம் மற்றும் சமச்சீரற்ற குறியீடு குறியாக்கம் வேறுபடாடுகளை எழுதுக.
3. குறிப்பு வரைக
   அ. எண்முறைச் சான்றிதழ்
   ஆ. எண்முறைக் கையொப்பம்
4. பாதுகாப்பான மின்னணு பரிவர்த்தனை (SET) மற்றும் அதன் செயல்பாடுகளை விளக்குக.
5. SSL மற்றும் அதன் பணிக் கோட்பாடுகளை விளக்குக.

மாணவர் செயல்பாடு

- குறிப்பிட்ட கட்டணம் செலுத்தும் முறையில் பயன்படுத்தப்படும் பாதுகாப்பு நெறிமுறைகளைப் இனங்காணுதல்.
- ஏதேனும் ஒரு பணம் செலுத்தும் முறையை பற்றி விளக்கப்படம் ஒன்றை உருவாக்கவும்.
- அந்த பணம் செலுத்தும் முறையில் பயன்படுத்தப்படும் பாதுகாப்பு தொழில்நுட்பத்தை விவரி.
- வேறு சில பணம் செலுத்தும் முறைக்கு செயல்பாடுகளை மீண்டும் செய்யவும்.

XII CompApp_Tamil version CHAPTER 17.indd 275 21-04-2020 12:29:32