அத்தியாயம் 1

மறைமுக மாற்று குறியீட்டு எழுத்தியல் - அறிமுகம்

அகிலா என்பவள் (Akila - கற்பனைப் பெயர்) சில தகவல்களை மற்றொருவருக்கு அதாவது பரத் என்பவருக்கு (Bharath - கற்பனைப் பெயர்) அனுப்புவதாக வைத்துக் கொள்வோம். இந்தத் தகவல் ரொம்பவும் இரகசியமானது என்பதால் பரத்தைத் தவிர மற்ற எவரும் பார்க்கவோ, படிக்கவோ அல்லது பார்த்து அதை மாற்றி அனுப்பவோ கூடாது என்று அகிலா நினைக்கிறாள். ஒரு அலுவலகத்தில் அதன் மேலாளர் ஒரு ஊழியரை வேலையிலிருந்து நீக்கி விட்டதாக ஒரு மின்னஞ்சல் அனுப்பும்போது அந்த மின்னஞ்சலை மற்ற எந்த ஊழியரும் பார்த்துவிடாமல் இருக்க விரும்புவார். இதுபோன்று அனுப்பும் தகவல்களை பெறுபவர் மட்டும் படித்துத் தெரிந்துக் கொள்ள, இந்த தகவலின் விவரத்தை மறைமுகமாக மாற்று எழுத்துகளில் எழுதி அனுப்புவதை மறைமுக மாற்று குறியீட்டு எழுத்தியல் அதாவது கிரிப்டோகிராஃபி (Cryptography) என்று அறியப்படுகிறது. புதுப் புது தொழில்நுட்பம், கணினி வளர்ச்சி தவிர தகவல் பரிமாற்ற முன்னேற்றம் காரணமாக பாதுகாப்பு கருதி கிரிப்டோகிராஃபி வழி தகவல் அனுப்ப முயற்சி மேற்கொள்ளப்பட்டது.

உலகத் தரம்வாய்ந்த மிகப்பெரிய நிறுவனம் ஒன்று பூட்டும், சாவியும் செய்து வியாபாரம் செய்ய விரும்பியது. அறிவும் திறமையும் உள்ள ஒரு இயந்திரவியல் பொறியாளரை (மெக்கானிக்கல் என்ஜினீயர் - Mechanical Engineer) வேலைக்கு அமர்த்தி, எளிதில் திறக்க முடியாத நல்ல பூட்டு, சாவியில்லாமல் வடிவமைத்தது. அதனுடைய உட்பாகத்தின் வடிவமைப்பு, பூட்டவும், திறக்கவும் செய்யும் விதத்தில் நடுவில் வளையம் ஒன்று அமைத்து, இந்த விவரத்தை அதை வாங்குபவருக்கு மட்டும் தெரிவித்து விற்கிறது. அவர்கள் வடிவமைத்த பூட்டின் நடுவில் உள்ள வளையத்தில் 1, 2, 3, ... 32 என்ற எண்கள் குறிப்பிட்டிருக்கும். பூட்டை பூட்டவோ, திறக்கவோ செய்ய, அந்த நடுவிலுள்ள வளையத்தை வலது புறமாகவும், இடது புறமாகவும் இத்தனை தடவை சுற்றும்படி வடிவமைத்திருக்கும். இந்த வடிவமைப்பு ரொம்பவும் பாதுகாப்பானது. அதை வடிவமைத்த பொறியாளருக்கும் கூட எளிதில் தெரிந்துகொள்ள முடியாத ஒன்று என்றால் மிகையில்லை.

படம் 1.1

இந்த வடிவமைப்பில் அந்த நிறுவனம் ஆயிரத்துக்கு மேல் பூட்டு (Lock without separate Key) விற்பனைக்காகத் தயாரித்தது. அகிலாவும், அந்த நிறுவனத்திலிருந்து பூட்டு ஒன்று விலைக்கு வாங்கி, அதை பூட்டவோ, திறக்கவோ செய்ய, வலது, இடது பக்கம் மாற்றி, மாற்றி சுற்றும் விதத்தை தனக்கு விருப்பமுள்ள எண்களில் மாற்றிவைத்துக் கொள்கிறாள். பூட்டை பூட்ட, திறக்க தேவையான சுழற்சி, வலது, இடது எத்தனை எண்கள் போன்ற விவரம் அகிலாவைத் தவிர, வேறு யாருக்கும், அந்த நிறுவனப் பொறியாளருக்கும் கூட அறியமுடியாது. அகிலா இந்தப் பூட்டை திறக்கும் சுழல் எண் விவரங்களை மறந்துவிட்டால், பூட்டை உடைப்பதைத் தவிர வேறு எந்த விதத்திலும் திறக்க முடியாது. இந்த நிறுவனத்திலிருந்து பரத் என்பவனும் ஒரு பூட்டை வாங்கி தனக்கேற்ற விதம் சுழல் எண்களை மாற்றிவைத்து கொள்கிறான். அகிலாவுக்கு பரத் வாங்கின பூட்டையோ அல்லது வேறு எவருடைய பூட்டையோ திறக்க இயலாது. அதுபோல பரத்துக்கு அகிலா வாங்கின பூட்டையோ அல்லது வேறு எவருடைய பூட்டையோ திறக்க இயலாது என்பது குறிப்பிடத் தக்கது. இதுபோன்ற பூட்டை அத்துமீறி வேறொருவன் அல்லது திருடன் பல தடவை சுழற்சி செய்து முயற்சித்தாலும் பூட்டு திறக்காது. சுழற்சி எண் 16, 24, 32 போன்ற எண்கள் உள்ள பூட்டை வாங்கினால் கூடுதல் பாதுகாப்புள்ளதாக இருக்கும். மற்றொருவரோ, திருடனோ சுழற்சி எண்களை ஊகித்து திறக்கும் நேரம் அதிகமாக இருக்க வேண்டுமானால், சுழற்சி எண் 40, 48, 64 போன்ற எண்கள் உள்ள பூட்டை வாங்குவது நல்லது.

அகிலா சில முக்கிய ஆவணங்களை ஒரு பெட்டியில் வைத்து அவள் வாங்கிய பூட்டினால் பூட்டி பெட்டியை பரத்துக்கு அனுப்புவதாக வைத்துக் கொள்வோம். பரத்துக்கு அந்தப் பெட்டி கிடைத்ததும் அதைத் திறக்கும் விதம் அகிலா அவனுக்கு சொன்ன பிறகுதான் பெட்டியைத் திறக்க முடியும். அகிலாவும் பெட்டியைத் திறக்கும் விதத்தை வேறு யாருக்கும்

தெரியாமல் பரத்துக்கு மட்டும் தெரியும்படி இரகசியமாகத்தான் சொல்லவேண்டும். வேறு யாராவது இந்தத் தகவலைத் தெரிந்துகொண்டால், அவர்களால் பெட்டியைத் திறந்து ஆவணங்களை எடுத்து பார்க்கவோ, படிக்கவோ முடியும்.

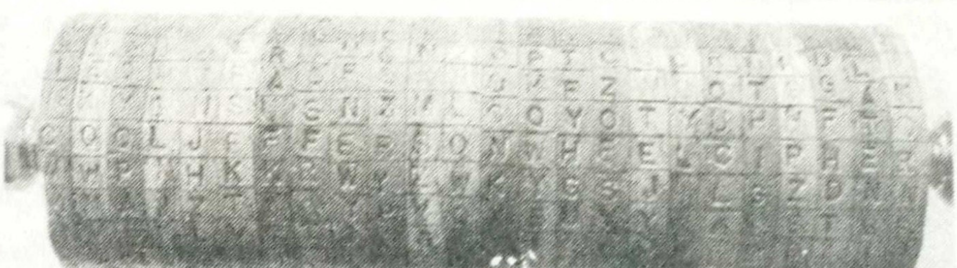
மறைமுக மாற்று குறியீட்டாக்கம் என்பதும் மேலே கூறியது போன்ற பூட்டும், அதை திறக்கும் சுழற்சி எண், வலது, இடது பக்கம் எத்தனை தடவை சுழற்றுதல் ஆகிய தகவல் போன்ற ஒன்றுதான். பலவிதமான வடிவமைப்பில் பூட்டும் திறக்கும் விதமும் இருப்பதுபோல, மறைமுக மாற்று குறியீட்டுக்கும் ஒழுங்குமுறை (மெத்தேடு - Method) வழிகள் உண்டு. பரத்தும் அகிலாவுடைய பூட்டை திறப்பதற்குள்ள வடிவமைப்புத் தகவல் தெரிந்து அவளுடைய பூட்டை வாங்கி தன்னுடைய பொருட்களை பெட்டியில் வைத்து பூட்டிவைத்தால், அகிலாவுக்கு அந்தப் பெட்டியின் பூட்டைத் திறந்து பெட்டியிலுள்ள பொருட்களைப் பார்க்க முடியும். இதேபோன்றதுதான் அகிலாவுக்கும் பரத்துக்குமிடையே ஒருவருக்கொருவர் தொடர்பு கொள்ளும் மின்னஞ்சல் (ஈமெயில் - Email) தகவல்களும். இந்த இருவரும் தொடர்புகொண்டு தகவல் அனுப்பும் போது, அந்தத் தகவலை மற்றொருவர், அதாவது அத்துமீறி செயல்படுபவரான நீலகேசி (கற்பனைப் பெயர்) என்ற இன்ட்ரூடர் (Intruder) பார்த்து படிக்காமலிருக்க, தகவல் எழுத்துகளை மறைமுக மாற்று குறியீடு எழுத்தாக எழுதி அனுப்புவதை சுருக்கமாக மறைமுக மாற்று குறியூட்டாக்கம் என்று சொல்லலாம். அதாவது பூட்டும் அதனுடைய திறவுகோலும் (கீ - Key) இணைந்தது தான் கிரிப்டோகிராஃபி. பலவிதமான பூட்டும், திறவுகோலும் இருப்பதுபோல் மறைமுக மாற்று குறியீடு எழுதுவதிலும் பலவகை செயல்முறைகள் இன்றும் நிலுவையில் உள்ளது. அகிலாவுடைய பூட்டும் சிறந்த வடிவமைப்பு செயல்முறையும் அதன் திறவுகோலும் அனுமதியில்லாத எவனும் திறந்து பார்க்க முடியாததாகவும், பாதுகாப்பானதாகவும் இருக்கும். அகிலா வடிவமைத்த செயல் முறையின் சரியான நகல் பரத்திடம் இருந்தால் மட்டும்தான் அவனுக்கு மறைமுக மாற்றுக் குறியீட்டு எழுத்துகளை அசல் எழுத்தாக மாற்றி படிக்க முடியும். இதேபோன்றதுதான் அகிலா, பரத் இருவருடைய தகவல், மின்னஞ்சல் தொடர்பு பாதுகாப்பான ஒன்றாக வடிவமைக்க வேண்டும்.

கிரிப்டோகிராஃபி என்பதும் இரகசியத் தகவல்களை உரிமையில்லாத மற்றொருவர் பார்த்து படிக்க, திருத்தி எழுத முடியாத விதத்தில் பாதுகாப்பாக தொடர்புகொள்ள வழி வகுக்கும். மறைமுக மாற்று குறியீட்டு எழுத்தாளர்கள் (கிரிப்டோகிராஃபர்ஸ் - Cryptographers) என்பவர் அசல் தகவல் எழுத்து உரையை (ப்ளெயின் டெக்ஸ்ட் - Plain text) மறைமுக மாற்று குறியீட்டு உரையாக எழுதுபவர்கள். அவர்கள் மாற்று எழுத்து குறியீடு எழுத உபயோகிக்கும் திறவுகோல் விவரம் யாருக்கு அவசியமோ அவர்களுக்கு மட்டும் தெரியப் படுத்துதல் மிக மிக அவசியம்.

மறைமுக மாற்று குறியீட்டு ஆய்வாளர் (கிரிப்ட் அனலிஸ்ட் - Crypt analyst) என்பவர் கணிதவியல் (mathematical) மொழியியலில் (Linguistic) திறமையுள்ளவராக

இருப்பார்கள். இவர்களுக்கு மறைமுக மாற்று குறியீட்டு எழுத்து தகவல்களை, அசல் எழுத்து தகவல்களாக மாற்றும் வழிமுறைகளை கண்டறிந்து படிக்கும் ஆற்றல், முயற்சி செய்வதில் உள்ள ஆர்வம் அதிகம் இருக்கும். மறைமுக மாற்று குறியீட்டு எழுத்துகளை அசல் எழுத்தாக மாற்றும் திறவுகோலை அயராது முயற்சி செய்து கண்டுபிடித்து இரகசியத் தகவல்களை அறிந்துகொள்ளும் திறமையாளர்களை மறைமுக மாற்று குறியீட்டு ஆய்வாளர் என்று கூறலாம். கிரிப்ட் (Crypt) என்ற வார்த்தை கிரேக்க மொழியின் கிரிப்டோஸ் (Kryptos) என்ற வார்த்தையிலிருந்து உருவானது. கிரிப்டோஸ் என்றால் மூடிவைப்பது, மறைத்தல் என்று அர்த்தம். பேசும் மொழியின் எழுத்துகள் உருவானபோதே, மொழியியல், கணிதவியல் அறிவு மிகுந்த புத்திசாலிகள் கிரிப்டோகிராஃபியிலும், கிரிப்ட் அனாலிஸிஸிலும் கவனம் செலுத்த முயன்றனர். இவர்களே பல புதிர்களை (puzzle) உருவாக்கவும் அதை விடுவிப்பதிலும் தங்கள் நேரத்தை செலவிட்டு வாழ்நாட்களை ஓட்டிவந்தனர். சுடோக்கு (Sudoku), புதிர்கட்டம் போன்றவை நாளேடு, பத்திரிகை, புத்தகம் ஆகியவற்றில் வருவதை பலரும் முயற்சி செய்து விளையாடுவதை இன்றும் நாம் கண் கூடாகக் காணலாம்.

மாற்று குறியீட்டு ஆய்வாளர் தங்கள் விடாமுயற்சியால் கிரிப்டோகிராஃபர்கள் அனுப்பும் தகவல்களை, அசல் எழுத்து தகவல் உரையாக (PlainText) மாற்றும் வழிமுறையை உருவாக்கி படிக்க முயலுவார்கள். கிரிப்டோகிராஃபர்கள் மாற்று குறியீட்டு ஆய்வாளர்களை விட ஒரு படி மேல் புகுந்து, புதிய வழிகளில் சாமர்த்தியமாக தகவல் எழுத்துகளை மாற்றி அமைப்பதில் கவனம் செலுத்தி இரகசியமாக தகவல்களை அனுப்ப முயற்சி செய்வார்கள். கணினிகள் (Computers) பெருமளவில் உபயோகத்திற்கு வந்ததும், பழைய வழிமுறைகளை எல்லாம் பின்தள்ளி, தற்கால தொழில் நுட்பம் வழியாக மறைமுக மாற்று எழுத்துகளை புதுப்புது முயற்சிகளால் உருவாக்கி வடிவமைக்கப்படுகிறது. கிரிப்டோகிராஃபியின் தந்தை என்று அழைக்கப்படும் அமெரிக்கர் தாமஸ் ஜெஃபர்சன் (Thomas Jefferson) என்பவரால் கண்டுபிடிக்கப்பட்ட உருளையை வீல் ஸைஃபர் (Wheel Cipher) என்ற கருவியே முதன் முதலாகக் கண்டுபிடிக்கப்பட்ட மாற்று எழுத்து குறியீட்டுக் கருவியாகும்.



படம் 1.2 Wheel Cipher

இன்றைய காலகட்டத்தில் மக்கள் பலரும் மின்னணு வலை அமைப்பு (எலக்ட்ரானிக் நெட்வொர்க் - Electronic network), இணையம் (இன்டர்நெட் - Internet)

வழியாக தகவல் பரிமாற்றம் செய்துவருகிறார்கள். இந்தத் தகவலை மறைமுக மாற்று குறியீட்டு எழுத்தாக மாற்றி எழுதாமல் பிறருக்கு அனுப்பும்போது, தேவையில்லாத பலரும், அதாவது அழையாத அத்துமீறி நுழைபவர்களும் (இன்ட்ருடர் - Intruder) எதிரிகளும் (ஹாக்கர் - Hacker), வேண்டாதவர்களும் (அட்வெர்ஸரி - adversary) அதைப் படிக்க நேரிடும். அதனால் இது போன்ற தகவலை இரகசியமாக யாருக்கு அனுப்ப வேண்டுமோ அவர்களுக்கு மறைமுக மாற்று குறியீட்டு எழுத்தில் எழுதி அனுப்பி, அதை அவர்கள் மட்டும் படிக்க வசதியாக, அசல் எழுத்து தகவலாக மாற்றும் திறவுகோலும் கொடுத்துவிட வேண்டும். இதற்கு கிரிப்டோகிராஃபி வழிமுறைகள் மிகவும் உதவியாக இருக்கும்.

நீங்கள் ஒரு வியாபார நிறுவனம் ஒன்றில் வேலை செய்பவராக இருக்கலாம். தினந்தோறும் உங்கள் நிறுவனம் எவ்வளவு வியாபாரம் செய்தது என்ற கணக்கு விவரம், விற்பனை அறிக்கை (ஸேல்ஸ் ரிப்போர்ட் - Sales Report) உங்கள் அலுவலக மேலதிகாரிக்கு மட்டும் இணையதளம் வழியாக அனுப்புகிறீர்கள் என்று வைத்துக் கொள்வோம். இந்த கணக்கு விவரம், உங்கள் அலுவலகத்தில் வேலை செய்யும் மற்றவர்களுக்கோ, அல்லது இணைய தளத்திலுள்ள விவரத்தை அனுமதியின்றி ஊடுருவிச் சென்று பார்ப்பவர் களுக்கோ தெரிந்தால், அது உங்கள் நிறுவனத்தை பெரிதும் பாதிக்கும். அது நாட்டு பாதுகாப்பிற்கு எதிரானது இல்லை என்றாலும், மற்ற போட்டி நிறுவனங்கள் உங்கள் நிறுவன விவரங்களைத் தெரிந்துகொண்டு, முன்னெச்சரிக்கையாக இருந்து அவர்கள் வியாபாரத்தை பெருக்க வழி வகுக்கும். அவசியமில்லாதவர்கள் பார்க்க முடியாமல் விவரத்தை அனுப்ப கிரிப்டோகிராஃபி மிகவும் பயனுள்ளதாக இருக்கும். கிரிப்டோகிராஃபி முறையால் ஒருவருக்கு தகவல் அனுப்பி அவர்கள் மட்டும் பார்த்து தெரிந்து கொள்ளும் வழியில் அனுப்ப முடியும்.

கிரிப்டோகிராஃபி பற்றி எல்லோரும், முக்கியமாக, தமிழ்படிக்கக் கூடியவர்கள் தெரிந்து கொள்ளவும், எந்தெந்த வழி முறைகளில் அது கையாளப்படுகிறது என்பதையும் தமிழில் எளிய முறையில் விரிவாக பின்வரும் அத்தியாயங்களில் எழுதியிருக்கிறேன். சில ஆங்கில வார்த்தைகளுக்கு இணையான தமிழ்ச் சொற்கள் நடைமுறையில் இல்லாததால் ஆங்கில வார்த்தைகள் எழுதியிருப்பது தவிர்க்க முடியாத ஒன்றாகிவிட்டது.

அத்தியாயம் 2

மாற்று எழுத்தும் (Substitution)

ஸீஸரின் ஸைஃபரும் (Caesar's Cipher)

ஒரு தகவலை ஒரு மொழியின் எழுத்துரு வழி எழுதுவதை அசல் எழுத்துத்தகவல் அல்லது எளிய உரை (Plain Text) என்று கூறலாம். இதை படிக்கவோ, படித்து தெரிந்துகொள்ளவோ எந்த வித கருவிகளோ, தனிப்பட்ட முயற்சியோ தேவையில்லை. இந்த அசல் எழுத்துத் தகவலை மறைமுக மாற்று குறியீடு வழிமுறையில் எழுதுவதை மறை குறியீடாக்கம் (என்கிரிப்ஷன் - Encryption) என்று சொல்லப்படுகிறது. மறை குறியீடாக்கம் செய்த ஒரு தகவலில் உண்மையான தகவல் எழுத்துருவை மறைத்து மாற்று குறியீடாக எழுதப் பட்டிருப் பதால் அதை எளிதில் எவரும் படித்து புரிந்துகொள்ள முடியாது. ஒரு அசல் எழுத்துத் தகவலை என்கிரிப்ஷன் செய்து மறைமுக மாற்று குறியீட்டுத் தகவல் ஆனதை, படித்து புரிந்துகொள்ள முடியாத தகவல் என்பதால், இதை மறை குறியீட்டுத் தகவல் (ஸைஃபர் டெக்ஸ்ட் - Cipher Text) என்று அழைக்கப்படுகிறது. இதுபோன்று என்கிரிப்ஷன் செய்த தகவலை மற்றவர்கள் பார்க்க முடியும் என்றாலும், அதில் என்ன எழுதியிருக்கிறது என்பதை எளிதில் படித்து புரிந்துகொள்ள முடியாது. மறை குறியீட்டுத் தகவலை மறுபடி ப்ளெயின் டெக்ஸ்ட் தகவலாக மாற்றுவதற்கு அசல் எழுத்தாக்கம் (டீக்கிரிப்ஷன் - decryption) என்று சொல்லப்படுகிறது. எவருக்கு ஒரு தகவலை தெரியப் படுத்த வேண்டுமோ அவர்களுக்கு மட்டும் மறை குறியீட்டுத் தகவலும், டீக்கிரிப்ஷன் செய்ய அதற்குரிய திறவுகோலும் அனுப்பினால் அவர்களால் மட்டும் மறை நீக்கி தகவலைப் படிக்க முடியும்.

மறைமுக மாற்று குறியீட்டு எழுத்தாக எழுதும் நெறிமுறை (அல்காரிதம் - algorithm) என்பது, ஒரு திறவுகோல், கடவுச்சொல் (password), இரகசிய எண்கள், வினைமுற்றுப் பெறாத சொற்றொடர் (passphrase) இவற்றால் அசல் தகவலை என்கிரிப்ட் செய்யும் ஒரு வழிமுறைதான். ஒரு அசல் தகவலை விதவிதமான திறவுகோல் உபயோகித்து பலவித மறை குறியீட்டுத் தகவலாக என்கிரிப்ட் செய்ய முடியும். என்கிரிப்ட் செய்த தகவலின் பாதுகாப்புக்கு (செக்யூரிட்டி - security) இரண்டு செயல்கள் மிக அவசியம். ஒன்று என்கிரிப்ட் செய்யும் வழிமுறையின் வலிமை (ஸ்ட்ரெத் - strength), இன்னொன்று வழிமுறையைக் கையாள உருவாக்கும் திறவுகோலை இரகசியமாக (ஸீக்ரஸி - secrecy) பாதுகாக்கும் திறன். மறைமுக மாற்று குறியீட்டு எழுத்தியல் வழிமுறையும், உருவாக்கும் திறவுகோலும், வழிமுறையைக் கையாள நிபந்தனைக்கு உட்பட்ட வரைமுறையும் (ப்ரோட்டகோல் - protocol) சேர்ந்த ஒன்றை குறியாக்கமுறை (Cryptosystem) என்று கூறப்படுகிறது.

ஆரம்பத்தில் பாரம்பரியமான பலவித ஸைஃபர் முறைகள் (ஸைஃபர் ஸிஸ்டம் - Cyber Systems) பயன்படுத்தப்பட்டிருந்தாலும் காலப்போக்கில்

அவை பிரபலமடையாமல் இரண்டாவது உலக மகா யுத்தம் வரை நிலவியிருந்தது என்று சொல்லலாம். கணினிகள் வந்த பிறகு அவ்வழிமுறைகள் முற்றிலுமாக கைவிடப் பட்டது. இருப்பினும் இரண்டுவித ஸைஃபர் வழிமுறைகள் இன்றும் நடைமுறையில் உபயோகத்தில் இருப்பதை மறுக்க முடியாது. ஒன்று எழுத்துருவை இடம் மாற்றி எழுதும் வகை (ட்ரான்ஸ்பொஸிஷன் ஸிஸ்டம் - Transposition System). இன்னொன்று, எழுத்துரு ஒன்றுக்கு பதில் வேறொரு எழுத்துரு எழுதும் வகை, அதாவது மாற்று எழுத்து வகை (ஸப்ஸ்டிட்யூஷன் ஸிஸ்டம் - Substitution System). முதலில் ஸப்ஸ்டிட்யூஷன் ஸிஸ்டம் பற்றி விரிவாகப் பார்க்கலாம்.

ஸீஸரின் ஸப்ஸ்டிட்யூஷன் ஸைஃபர்

Ceasar's Substitution Cipher

ஒரு போரில் (வார் - War) எதிரிகளை தோற்கடித்து வெற்றி பெற, போர்த் தலைவர்களிடையே தகவல் பரிமாற்றங்கள் மிகமிக இரகசியமாக இருத்தல் அவசியம். ஜூலியஸ் ஸீஸர் (Julius Caesar) தன் போர் தலைவர்களுக்கு தகவல்கள் அனுப்பும் போது அந்த தகவல் எதிரிகள் படித்து தெரிந்து கொள்ள முடியாதபடி மாற்று எழுத்து முறையில் அனுப்பியதாகத் தெரிகிறது. இந்த மறைமுக மாற்று எழுத்து வழிமுறையை ஸீஸர்ஸ் ஸைஃபர் (Caesar's Cipher) என்று அழைத்தனர். இந்த வழிமுறை வெகு எளிதில் தகவல் பரிமாற்றம் செய்ய உதவியது. இது ஒரு பாதுகாப்பான முறையில் உள்ளது என்று கூற முடியா விட்டாலும், முதன் முதலாக நமக்கு அறிமுகமான ஒரு மாற்று எழுத்து வழிமுறை என்று சொல்லலாம். போர் முனையில் இருக்கும் தம் படைத்தலைவனுக்கு ''அதிகாலை நான்கு மணிக்கு எதிரிகளை தாக்கச் செல்லவும்'' அதாவது ''அட்டாக் ஃபோர் ஏஎம்'' ("ATTACK FOUR AM") என்ற தகவலை அனுப்புவதாக எடுத்துக் கொள்வோம். ஒவ்வொரு ஆங்கில எழுத்துக்கு பதிலாக அந்த எழுத்திலிருந்து மூன்றாவது எழுத்து எதுவோ அதை எழுதி தகவலை அனுப்பி வைத்தார். மூன்று என்பது இங்கு திறவுகோலாகும். இந்த தகவலைப் படிப்பவர்களுக்கு அசல் தகவல் என்ன என்பது எளிதில் தெரிய வழியில்லை. ஒரு எழுத்துக்கு பதில் வேறொரு மாற்று எழுத்தை எழுதுவதால் இதை ஸப்ஸ்டிட்யூஷன் ஸைஃபர் என்று அழைக்கப் பட்டது.

Plain Letters	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphered Letters	D	E	F	G	H	I	J	K	L	M	N	O	P

Plain Letters	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphered Letters	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

மேற்கூறிய மாற்று எழுத்துப் பட்டியல்படி A என்பது D ஆகவும், T என்பது W ஆகவும்.

C என்பது F ஆகவும், ஒவ்வொரு எழுத்தையும் மாற்றி எழுதி தகவல் அனுப்பபட்டது. மறைமுக மாற்று எழுத்துப்படி, ''ATTACK FOUR AM'' என்பதை ''DWWDFN IRXU DP'' என்ற தகவலாக அனுப்பப்பட்டது. எதிரிகள் இதை படிக்கும்போது, எளிதில் இதன் அசல் எழுத்துத் தகவல் என்ன என்பதை தெரிந்து கொள்ள முடியாது. படைத் தலைவனுக்கு இந்த தகவல் அனுப்பும் போது, இதை அசல்குறியீடாக்கம் செய்துபடிக்க, ''3'' என்ற திறவுகோலையும் (Key) தனியாகத் தெரிவிக்க வேண்டும். ஒவ்வொரு தடவையும் தகவல் அனுப்பும்போது, 3-க்கு பதில் 5, 7, 9 ஆகவுள்ள மாற்று எழுத்து எழுதி என்கிரிப்ட் செய்த தகவலையும், எந்த திறவுகோல் (5, 7, 9) உபயோகிக்க வேண்டும் என்ற விவரமும் படைத்தலைவனுக்கு இரகசியமாக அனுப்ப வேண்டும். இந்த வழிமுறையில், ப்ளெயின் டெக்ஸ்டு ஆன "SECRET" (ஸீக்ரெட்) என்ற வார்த்தையை Key 3 (மூன்றாவது எழுத்து) வைத்து மாற்று குறியீட்டாக்கம் செய்தால் "VHFUHW" என்ற ஸைஃபர் டெக்ஸ்டு வார்த்தையாகிவிடும்.

நேரடியான மாற்று எழுத்து வழி, எழுத்துகளை மாற்றி எழுதுவதை ஸீஸர்ஸ் ஸப்ஸ்டிட்யூஷன் ஸைஃபர் என்று உரோமன் (Roman) நாட்டு அரசர் ஜூலியஸ் ஸீஸர் (Julius Caesar) பெயரில் அழைக்கப்பட்டது. ஒரு குறிப்பிட்ட அசல் தகவல் எழுத்திலிருந்து ஒரு குறிப்பிட்ட எண்ணில், அதாவது மூன்றாவது அல்லது ஐந்தாவது (இந்த எண் தான் திறவுகோல்) ஆக இருக்கும் மற்றொரு எழுத்தை மாற்றி எழுதுவதால் ஸப்ஸ்டிட்யூஷன் என்று கூறுகிறோம். இருபத்தியொன்றாவது எழுத்துக்கு மாற்றி எழுதினால் ஸைஃபர் டெக்ஸ்ட் எப்படி இருக்கும் என்று பார்ப்போம்.

அசல் ஆங்கில எழுத்து வரிசை:

(வரிசை 1) 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

21ஆவதாக இருக்கும் ஸப்ஸ்டிட்யூஷன் ஆங்கில எழுத்து வரிசை:

(வரிசை 2) 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

ப்ளெயின் டெக்ஸ்ட் - MEET ME TOMORROW

ஸைஃபர் டெக்ஸ்ட் - HZZO HZ OJHJMMJR

கணித முறைப்படி ஸைஃபர் டெக்ஸ்ட் எழுத்தை கண்டுபிடிப்பது எப்படி என்று பார்ப்போம். அசல் வரிசையான ப்ளெயின் டெக்ஸ்ட் ஆங்கில எழுத்தையும், ஸைஃபர் டெக்ஸ்ட் ஆங்கில எழுத்தையும் முறையே i and j என்று வைத்துக் கொண்டால் மேலே காட்டிய உதாரணத்தில்,

i = 1, 2, 3, . . . 26 என்ற எண் வரிசை, $j = i + 21 \pmod{26}$ என்ற எண்ணைக் குறிக்கும். mod 26 என்பது $i + 21$ எண்ணை 26 ஆல் வகுத்துக் கிடைக்கும் மீதி எண் (Remainder).

கிரிப்டோகிராஃபிக் வழிமுறைகளில் மாடுலர் கணித (Modular Math) முறை பயன்படுத்துகின்றன. வகுத்தல் (division method) வழிமுறையே Modular Maths ல் அதிகமாக உபயோகிக்கப் படுகிறது. ஆரம்ப பள்ளியில் நமக்கு தெரிந்த கணக்கு.

Quotient + Remainder

Divisor | Dividend (residue)

(modulus)

நாம் அன்றாடம் நேரம் கண்டுபிடிக்க மாடுலர் செயல்பாடு வழி (Modular operations) செய்து பார்க்கிறோம். 10 மணி + 5 மணிக்கூர் என்பது மதியம் 3 மணியைக் குறிக்கும். Modular Math வழி சொல்வதென்றால் (10 + 5) mod 12 = 3. Modulo என்பதை சுருக்கமாக mod என்று எழுதுவர். 21mod10=1, அதாவது வகுபடும் எண் (டிவிடெண்ட் - dividend) 21ரை 10 - ஆல் வகுக்குபோது கிடைக்கும் மீதி எண் 1. இங்கு 10 என்ற வகுக்கும் எண்ணை (டிவைசர் - divisor) அல்லது மாடுலஸ் (modulus) என்றும், மீதி 1 என்ற ரிமைன்டரை (remainder) ரெஸிடியூ (residue) என்றும் அழைக்கப்படுகிறது.

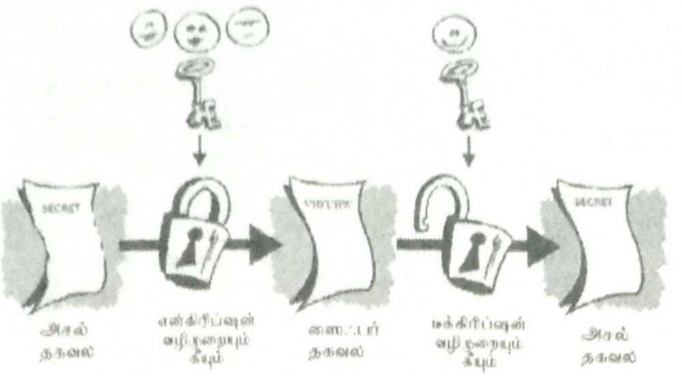
2 remainder 1

10 | 21 (residue)

(modulus)

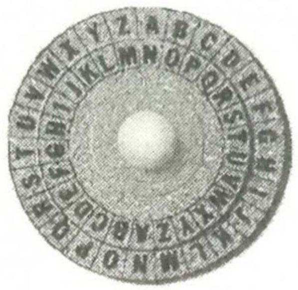
ஆங்கில எழுத்து வரிசையில் M என்பது 13 ஆவது எழுத்து. இதற்குரிய மாற்று எழுத்து வரிசை எண் (j) கிடைக்க 13 + 21 (mod 26). அதாவது 34 mod 26 = 34/26 , மீதி (remainder) 8 ஆகும். அதனால் மாற்று எழுத்து 1-வது வரிசையிலுள்ள 8 -வது எழுத்து H சைக் குறிக்கும். அதே போல் T என்பது ஆங்கில எழுத்து வரிசையில் 20 வது எண். இதற்குரிய மாற்று எழுத்து எண் கண்டுபிடிக்க 20 + 21 (mod 26) = 41 (mod 26) = 15, அதனால் 15 வது எழுத்து ''O'' என்பது மாற்று எழுத்தாகும்.

ஸீஸர் ஸப்ஸ்டிட்யூஷன் வழிமுறையில் ஆங்கில எழுத்து வரிசையில் (ஆர்டர் ஆஃப் தி லெட்டர்ஸ் - order of the letters) எந்த மாற்றமும் இல்லை என்பது முக்கியமான ஒன்று. இந்த வழிமுறைப்படி ஸைஃபர் டெக்ஸ்டு ஆக மாற்றுவதற்கு மொத்தமாக 25 Key தான் இருக்கமுடியும் என்பதை தெரிந்துகொள்ளவும். இதன் காரணமாக எதிராளிக்கு ஸைஃபர் டெக்ஸ்டைப் Plain டெக்ஸ்டாக எழுதிப் படிக்க மிக எளிது என்பது குறிப்பிடத்தக்கது. ஆங்கில வார்த்தைகளில் E என்ற எழுத்து, வார்த்தைகளில் மிக அதிகமாகப் பயன்படுத்துவதால் அதனுடைய மாற்று எழுத்தை எளிதாகக் கண்டுபிடித்து கீயைத் தெரிந்து கொள்ளமுடியும். மேலே கூறிய வார்த்தைகளில் E என்ற 5-ஆவது எழுத்துக்கு Z என்ற 26 - ஆவது மாற்று எழுத்து எழுதப்பட்டிருப்பதால், 26 - 5 = 21 என்பது கீயாக உபயோகித்து இந்த மாற்று எழுத்து எழுதப்பட்டிருக்கிறது என்று எளிதில் தெரிந்துகொள்ள முடியும்.



படம் 2.1 என்கிரிப்ஷன்/டீக்கிரிப்ஷன்

சைஃபர் டெக்ஸ்ட் வார்த்தையின் (VHFUHW) எழுத்துகளை 23 என்ற திறவுகோல் கொண்டு டீக்கிரிப்ஷன் செய்தால் ப்ளெயின் டெக்ஸ்ட் வார்த்தை (SECRET) என்று கிடைத்து விடும். படம் 2.1 இல் பார்க்கவும்.



FRPERG

படம் 2.2 சைஃபர் கீ 13, SECRET என்ற வார்த்தையின் என்கிரிப்ட் செய்த வார்த்தை

படம் 2.2 இல் அசல் எழுத்து வரிசையையும், திறவுகோல் 13 உபயோகிக்கும் போது வரும் எழுத்து வரிசையையும் இரண்டு வட்டத் தகடுகளுக்குள் காட்டப் பட்டிருக்கிறது. உள்வட்டத் தகடு திறவுகோல் எண் 13 என்ற வரிசை எண்படி சுற்றி வைத்திருக்கிறது. ''SECRET'' என்ற ப்ளெயின் டெக்ஸ்ட் ''FRPERG'' என்ற சைஃபர் டெக்ஸ்ட் வார்த்தையாக மாற்றியதைக் காட்டுகிறது. வெளி வட்டத் தகடில் ப்ளெயின் டெக்ஸ்டு வரிசையாகவும், உள் வட்டத் தகடை எந்த திறவுகோல் (கீ) எண்படி வேண்டுமோ அதன்படி சுழற்றி வைத்து சைஃபர் டெக்ஸ்டாக எழுத்துகள் மாற்றிக்காட்ட முடியும். திறவுகோல் எண் 25-க்கு பிறகு சைஃபர் டெக்ஸ்ட் எழுத்து மறுபடியும் 0 (பூஜ்யம்) ஆகிவிடுவதால் ப்ளெயின் டெக்ஸ்டு எழுத்தும், சைஃபர் டெக்ஸ்ட் எழுத்தும் ஒரே மாதிரி ஆகிவிடும். உள் வட்டத் தகடில் ஆங்கில எழுத்துகள் வரிசையாக இருப்பதால், மாற்று எழுத்து சைஃபர் டெக்ஸ்ட், உள்

வட்டத் தகடை எத்தனை கீ எண்ணுக்கு திருப்புகிறோமோ (ரொட்டேட் - rotate) அதன்படி தான் இருக்கும்.

ஆங்கில எழுத்தில் ''E'' என்ற எழுத்து வார்த்தைகளில் அதிகமாக வரக்கூடிய ஒன்று. அதற்கு அடுத்தாக கூடுதலாக வரும் எழுத்து ''T'' என்ற எழுத்து. இதைப் போன்று ஒவ்வொரு எழுத்தின் அதிர்வு எண்ணை (ஃப்ரீக்வென்ஸி - Frequency) வைத்து மற்றவர்கள் முக்கியமாக ஹாக்கர்ஸ் அல்லது அனுமதி யில்லாதவர்கள் ஸைஃபர் டெக்ஸ்டிலிருந்து ப்ளெயின் டெக்ஸ்டாக மாற்றி படிக்க எளிதில் முடியும்.

ஆங்கில எழுத்துக்களின் அதிர்வு எண் (English Letters Frequency)

A	B	C	D	E	F	G	H	I	J	K	L	M
73	9	30	44	130	28	16	35	74	2	3	35	25

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	74	27	3	77	63	93	27	13	16	5	19	1

ஒழுங்கு முறையையும் (மெத்தேடு - Method), திறவுகோலையும் தனியாகப் பிரித்து வைப்பது மிக முக்கியமான ஒன்று. புதிய வழிமுறைகளைப் பற்றித் தெரிந்து கொள்வதற்கு முன், ஸீஸருடைய ஸப்ஸ்டிட்யூஷன் ஸைஃபரின் வேறு வழிமுறை பற்றிப் பார்ப்போம். ஸீஸர் ஸைஃபர் வழிமுறையில் மாற்று குறியீட்டாக்கம் செய்ய, உள்வட்டத் தகடின் ஆங்கில எழுத்து வரிசையை 1 முதல் 25 வரை எந்த கீ வேண்டுமோ அந்த நம்பருக்குள்ள எழுத்தை மேல் வட்டத் தகடின் A என்ற எழுத்துக்கு கீழே வரும்படி வைக்கவும். மேல்வட்டத் தகடின் ஆங்கில எழுத்துக்கு (அசல் எழுத்து) நேராக வரும் உள் வட்ட தகடில் வரும் எழுத்து தான் ஸைஃபர் டெக்ஸ்ட் எழுத்து. இவ்விதம் பார்ப்பதை ஒழுங்குமுறை என்று சொல்லலாம். ப்ளெயின் டெக்ஸ்டில் மேல்வட்டத் தகடு எழுத்து A - க்கு பிறகு எத்தனை எழுத்துக்கு பிறகு உள்ள எழுத்து கீழ் வட்டத் தகடில் ஸைஃபர் டெக்ஸ்டாக எடுத்துக் கொள்ள வேண்டுமோ அந்த எண்தான் திறவுகோல் (Key) என்று சொல்லலாம். ஊடுருவிச் சென்று படிப்பவர்க்கு ஸைஃபர் டெக்ஸ்ட் என்கிரிப்ஷன் வழிமுறை தெரிந்தாலும், அதனுடைய மாற்று எழுத்து கீ (Key) தெரியவில்லை என்றால் அதனுடைய அசல் எழுத்து தகவலை கண்டுபிடிப்பது அவ்வளவு எளிதில்லை. இதனால் கீயை ரொம்ப பாதுகாப்பாக வைத்திருப்பது மிக முக்கியம்.

படம் 2.3

படம் 2.3 இல் அசல் எழுத்து வரிசையையும், திறவுகோல் 19 உபயோகிக்கும்போது வரும் எழுத்து வரிசையையும் இரண்டு வட்டத் தகடுகளுக்குள் காட்டப்பட்டிருக்கிறது. உள் வட்டத் தகடு திறவுகோல் எண் 19 என்ற வரிசை எண்படி சுற்றி வைத்திருக்கிறது.

படம் 2.4

(உள் வட்டத் தகடில் எழுத்துகள் வரிசையில் இல்லை)

அகிலா பரத்துக்கு படம் 2.4 இல் காட்டியபடி இரண்டு ஸைஃபர் வட்டங்களையும் அவள் அனுப்ப வேண்டிய அசல் தகவலை மறைமுக குறியீடாக்கம் செய்யும் கீயையும் கொடுப்பதாக வைத்துக் கொள்வோம். இரண்டு ஸைஃபர் வட்டங்களிலும் வெளிவட்டத் தகடில் ஆங்கில எழுத்து A, B, C, . . . Z என்ற வரிசையிலும், உள்வட்டத் தகடில் ஆங்கில எழுத்து, ஆல்ஃபபெட்டிக் வரிசைமுறைப்படி இல்லாமல் எழுத்துகள் மாறி மாறி வரும் முறையிலும் (ராண்டம் ஆர்டர் - random order) இருக்கும்.

Plain Letters	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphered Letters	Y	C	X	D	W	E	V	F	U	G	T	H	S

Plain Letters	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphered Letters	I	R	J	Q	K	P	L	O	M	N	A	Z	B

உள் வட்டத் தகடில் (ஸைஃபர் டெக்ஸ்ட்) ஆங்கில எழுத்து வரிசைப்படி இல்லாததால் இன்ட்ருடர்களுக்கு மாற்று எழுத்து எந்த அசல் எழுத்துக்காக எழுதப்பட்டிருக்கிறது என்பதை உடனடியாக கண்டுபிடிப்பது மிகக் கடினம். உள் வட்டத்தில் இப்படி வரிசை மாற்றி எழுதுவது நம்மால் நினைத்துப்பார்க்க முடியாத அளவு, கணக்கில் அடங்காத கோடிக்கணக்கான வழிகளில் எழுதமுடியும். ஸீஸர் ஸைஃபரில் ஒவ்வொரு எழுத்துக்கும் வெவ்வேறு மாற்று எழுத்து எழுதுவதால் இதை தனித்த அகர வரிசை ஸைஃபர் (மோனோ ஆல்ஃபபெட்டிக் ஸைஃபர் - Mono Alphabetic Cipher) என்று அழைப்பதுண்டு. இன்றைய மதிப்பளவுக்கு (ஸ்டான்டர்டு - Standard), ஸீஸர் ஸைஃபர் அவ்வளவு பாதுகாப்பானது இல்லையென்றாலும் முதன் முதலில் வழக்கமான கிரிப்டோகிராஃபி (கன்வென்ஷனல் கிரிப்டோகிராஃபி - conventional cryptography) எவ்விதம் உருவாக்கி உபயோகிக்கப்பட்டது என்பதற்கு ஒரு நல்ல உதாரணமாக எடுத்துக் கொள்ளலாம். இதில் பாதுகாப்பு அவ்வளவாக இல்லை என்பது தான் இதனுடைய பெரிய பலவீனம் (வீக்னஸ் -weakness) .

அத்தியாயம் 3

இடம் மாற்று ஸைஃபர் (Transposition Cipher)

இடம் மாற்று ஸைஃபரை, அசல் தகவலிலுள்ள ஆங்கில எழுத்தின் இடத்தை மாற்றி எழுதி ஸைஃபர் டெக்ஸ்டாக ஆக்குவது என்று சுருக்கமாகச் சொல்லலாம். ஒரு தகவலிலுள்ள ஆங்கில எழுத்துக்களை மாற்றாமல், அதன் ஒவ்வொரு எழுத்தின் இடத்தையும் மாற்றிவைத்து எழுதுவதுதான் இடம் மாற்று ஸைஃபர் (ட்ரான்ஸ்பொஸிஷன் ஸைஃபர் - Transposition Cipher) ஆகும். ஒரு வார்த்தையில் குறிப்பாக n எழுத்துகள் இருப்பதாகவும் அதை எப்படி இடம் மாற்றி எழுதி குறியீடு வார்த்தை ஆக்கலாம் என்று இனி பார்ப்போம்.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & . & . & . & n \\ i_1 & i_2 & i_3 & i_4 & . & . & . & i_n \end{pmatrix}$$

முதலாவது ப்ளெயின் டெக்ஸ்ட் எழுத்து i_1 என்ற இடத்துக்கும், 2ஆவது எழுத்து i_2 என்ற இடத்துக்கும், . . . கடைசி (n) எழுத்து i_n என்ற இடத்துக்கும் ஸைஃபர் டெக்ஸ்டில் மாற்றி எழுதப்பட்டிருக்கும். மேலே காட்டிய முதல் வரிசை (ரோ - Row) யிலுள்ள எண்கள் ஆல்ஃபபெட்டிக் வரிசைப்படியானதும், ரெண்டாவது வரிசையிலுள்ள எண்கள் வரிசைப்படி இல்லாமல் வேறுபட்ட வரிசை முறையிலும் (டிஃபெரன்ட் ஆர்டர் - different order) இருக்கும். மேற்கூறிய இரண்டு வரிசையையும் சேர்த்து சொல்லும்போது இது ஒரு n டிகிரி பெர்ம்யூட்டேஷன் (n degree Permutation) என்றாகிறது. பெர்ம்யூட்டேஷன் என்பது பலவிதத்தில் வரிசைமாற்றம் செய்வதைக் குறிக்கிறது.

இடம் மாற்று ஸைஃபரும் அதனுடன் சேர்ந்த வரிசை மாற்றமும் தெரிந்தால் நமக்கு எளிதாக என்கிரிப்ஷன், டீகிரிப்ஷன் செய்ய முடியும். அது எப்படி என்று பார்ப்போம்.

வரிசை மாற்றம் (1 2 3 4 5 6)

(Permutation) (5 2 3 6 1 4)

''READER'' என்ற ப்ளெயின் டெக்ஸ்ட் வார்த்தையை மேலே காட்டிய வரிசை மாற்றுப்படி என்கிரிப்ஷன் செய்தால் நமக்கு ''EEARRD'' என்ற ஸைஃபர் டெக்ஸ்ட் வார்த்தை கிடைக்கும். இந்த ஸைஃபர் டெக்ஸ்ட் வார்த்தையின் எழுத்துகளை 5 2 3 6 1 4 என்ற இடத்துக்கு மாற்றி எழுதினால் நமக்கு ப்ளெயின் டெக்ஸ்ட் வார்த்தை ''READER'' என்பது கிடைத்துவிடும்.

இதே வரிசை மாற்றம் உபயோகித்து ''OETDMH'' என்ற ஸைஃபர் டெக்ஸ்ட் வார்த்தையை அசல் எழுத்து வார்த்தையாகப் படிக்க நமக்கு கிடைப்பது ''METHOD''. அதேபோல் ''DESIGN''என்ற ப்ளெயின் டெக்ஸ்ட் வார்த்தை இந்த Permutation கொண்டு என்கிரிப்ஷன் செய்தால் நமக்கு ''GESNDI'' என்ற ஸைஃபர் டெக்ஸ்ட் வார்த்தை கிடைக்கும்.

(1 2 3 4 5 6)

(. . . . . .)

(5 2 3 6 1 4)

இரண்டாவது வரிசையில் உள்ள எண்கள் 6 ஐயும் கணிதவியல் இன்டக்ஷன் (mathematical induction) படி 6! (6 factorial) times அதாவது 6 * 5 * 4 * 3 * 2 * 1 = 720 வழிகளில் மாற்றி எழுதமுடியும். ப்ளெயின் டெக்ஸ்ட் எழுத்துகளை 720 வழிகளில் ஸைஃபர் டெக்ஸ்டாக ட்ரான்ஸ்பொஸிஷன் வழியில் மாற்றி எழுதமுடியும். n-letters உள்ள டெக்ஸ்டை 1, 2, 3, . . . n எண்களுக்குள்ள இரண்டாவது வரிசையை n! அதாவது n * (n-1) * (n-2) * . . . * 3 * 2 * 1 times வழிகளில் இடம் மாற்று ஸைஃபர் வழியில் குறியீடாக்கி எழுதமுடியும் என்று கூறலாம். n என்ற எண்ணின் மதிப்பு (வால்யு-value) கூடக்கூட, n! இலும் பெரிய எண்ணாக இருக்கும். முதல் 10 எண்களுக்குள்ள n! value எவ்வளவு என்பது கீழே தரப்பட்டிருக்கிறது.

n	1	2	3	4	5
n!	1	2	6	24	120

n	6	7	8	9	10
n!	720	5040	40320	362880	3628800

இரண்டாவது வரியிலுள்ள எண்களின் வரிசை, ஒரு வரிசை முறையின்றி சீரற்ற பெர்ம்யூட்டேஷன் (Random permutation) படி எழுதும்போது அதை நினைவில் வைத்துக் கொள்ளவோ, அல்லது ப்ளெயின் டெக்ஸ்ட், ஸைஃபர் டெக்ஸ்ட், தவிர சீரற்ற 2ஆவது வரிசை எண்களை யாருக்கு அனுப்ப வேண்டுமோ அவர்களுக்கு அனுப்ப எளிதாக இருக்காது. அதனால் ப்ளெயின் டெக்ஸ்ட் எழுத்துகளை எழுதும் வழியில் அதாவது Write-in path வழியிலும் ஸைஃபர் டெக்ஸ்ட் எழுத்துகளை வடிவியல் உருவமாகவும் (ஜியோமெட்ரிக்கல் ஃபிகர் - geometrical figure) எழுத முடியும்.

இந்த வழிமுறையை செல்வழி ட்ரான்ஸ்பொஸிஷன் (Route Transposition) என்று அழைக்கப்படுகிறது. உதாரணமாக, ஒரு நீள் சதுரம் (செவ்வகம் - rectangle) படத்தை சதுரக் கட்டங்களாக (ஸ்கொயர் ஸெல் - Square Cell) பகுத்துவைக்க வேண்டும். அந்த சதுரக் கட்டங்களுக்குள் ப்ளெயின் டெக்ஸ்ட் எழுத்துகளை மேலிருந்து கீழாகவோ, கீழிருந்து மேலாகவோ, முதல் வரி இடமிருந்து வலமாகவும், இரண்டாவது வரி வலமிருந்து இடமாகவும், மூன்றாவது வரி இடமிருந்து வலமாகவும் எழுதி, ஸைஃபர் டெக்ஸ்டாக எழுதும் போது அந்த செவ்வக சதுரக்கட்டம் எழுத்துகளை நெடு வரிசைப்படி (காலம் - column) எழுதிவிட வேண்டும். இப்படி எழுதும்போது நீலகேசி போன்ற அனுமதி யில்லாதவர்களுக்கு, ஸைஃபர் டெக்ஸ்டை ப்ளெயின் டெக்ஸ்டாக மாற்றிப் படிக்க மிகக் கடினம். இதை விளக்குவதற்கு, சில ப்ளெயின் டெக்ஸ்ட் கட்டங்களிலுள்ள எழுத்துகள் ஸைஃபர் டெக்ஸ்ட் எழுத்துகளாக எழுதிய பலவித வழிமுறைகளை கீழே காணலாம்.

"SHE HAS JUMPED IN A DEEP WELL TODAY" என்ற ப்ளெயின் டெக்ஸ்டை 4 * 7 கட்டத்தில் எழுதியதைப் பார்ப்போம்.

S	H	E	H	A	S	J
N	I	D	E	P	M	U
A	D	E	E	P	W	E
Y	A	D	O	T	L	L

படம் 3.1 Transposition Table

(Letters written horizontally from left to right, next right to left and so on)

இதனுடைய 6 விதமான ஸைஃபர் டெக்ஸ்ட் வார்த்தைகள் பின் வருமாறு:

SNAYADIHEDEDOEEHAPPTLWMSJUEL
JUELLWMSAPPTOEEHEDEDADIHSNAY
SNAYHIDAEDEDHEEOAPPTSMWLJUEL
JUELSMWLAPPTHEEOEDEDHIDASNAY
JSAHEHSUMPEDINEWPEEDALLTODAY
JSAHEHSNIDEPMUEWPEEDAYADOTLL

முதலிலுள்ள ஸைஃபர் டெக்ஸ்டை எப்படி ப்ளெயின் டெக்ஸ்டாக மாற்றுவது என்று பார்ப்போம். இது 7 Columnமும் 4 Rowவுள்ள கட்டம் என்பதை தெரிந்து கொள்ளவும். ஸைஃபர் டெக்ஸ்டிலுள்ளதை 4, 4 எழுத்துகளாகப் பிரித்துக் கொள்ளவும். முதல் 4 எழுத்தை கட்டத்தின் முதல் Column இல் மேலிருந்து கீழாக எழுதவும். அடுத்த 4 எழுத்தை கட்டத்தின் இரண்டாவது Column இல் கீழிருந்து மேலாக எழுதவும். படம் 3.2 ஐப் பார்க்கவும்.

S	H	E				
N	I	D				
A	D	E				
Y	A	D				

படம் 3.2

இதுபோல் அடுத்தடுத்த Column களில் அடுத்த 4 எழுத்துகளை எழுதவும். எழுதி முடித்ததும், படம் 3.1 இல் உள்ளதுபோல் வரும். இதில் முதல் Row வில் இடமிருந்து வலமாகவும், அடுத்த 2 ஆவது Row வில் வலமிருந்து இடமாகவும், அடுத்த 3 ஆவது Rowவில் இடமிருந்து வலமாகவும் முறையே வரிசையாக எழுதினால் ''SHE HAS JUMPED IN A DEEP WELL TODAY'' என்ற ப்ளெயின் டெக்ஸ்ட் கிடைத்து விடும்.

இன்னொரு உதாரணம்: "SHE MUST COMPLETE THE WORK BY NITE"

T	S	U	M	E	H	S
C	O	M	P	L	E	T
R	O	W	E	H	T	E
K	B	Y	N	I	T	E

படம் 3.3 Transposition Table

(Letters written horizontally from right to left, next left to right and so on)

இதனுடைய ஸைஃபர் டெக்ஸ்ட்

"STEETTEHELHINEPMUMWYBOOSTCRK"

(இன்ட்ரூடருக்கு சிறிது கஷ்டமாக இருக்கும் விதமாக NIGHT என்ற வார்த்தையை NITE என்று எழுதியிருப்பதை கவனிக்கவும்).

இன்னொரு உதாரணம்:

Plain Text "LAST EVENING WENT TO SHOPPING ALONE"

L	A	S	T	E	V
E	N	I	N	G	W
E	N	T	T	O	S
H	O	P	P	I	N
G	A	L	O	N	E

படம் 3. 4 Transposition Table

(Letters written horizontally from left to right)

Encryption Message:
"LEEHGANNOASITPLTNTPOEGOINVWSNE"

இங்கு எழுத்துகள் மேலிருந்து கீழாக மாற்றுக் குறியீட்டு எழுத்தாக எடுத்து எழுதியிருக்கிறது. மேலே உள்ள 5 * 6 கட்டத்தில் ப்ளெயின் டெக்ஸ்டின் எழுத்துகளை ஒவ்வொரு row விலும் இடமிருந்து வலமாக எழுதியிருக்கிறது. இதை ஸைஃபர் டெக்ஸ்டாக என்கிரிப்ட் செய்யும்போது முதல் column இல் மேலிருந்து கீழாகவும் அதன் பிறகு இரண்டாவது column இல் மேலிருந்து கீழாகவும் மற்ற column களிலிருந்தும் இது போல் எழுத்துகளைச் சேர்த்து எழுதியதைக் காணலாம். இந்தத் தகவல் யாருக்கு அனுப்ப வேண்டுமோ, அவர்களுக்கு Grid கட்டத்தின் நீளம், வீதியும் (length, breadth), அதாவது எத்தனை column, எத்தனை row என்பதும், ப்ளெயின் டெக்ஸ்ட் எழுத்துகள் எந்த வழியில் கட்டத்திற்குள் எழுதப்பட்டிருக்கிறது என்ற விவரமும், மறைமுக மாற்று குறியீட்டு தகவலுடன் தெரிவிக்க வேண்டும்.

மாற்றுக் குறியீட்டு ஆய்வாளர் ஸைஃபர் டெக்ஸ்டின் முன்மாதிரியைப் (பேட்டர்ன் - pattern) புரிந்துகொண்டு அதற்கேற்ப எழுத்துகள் என்னென்ன வரும் என்பதை ஊகித்து கண்டுபிடிக்க முயற்சிப்பார்கள். தவிர ஆங்கிலத்தில் e, t போன்ற எழுத்துகள் அதிகமாக வருவதும், இரண்டு எழுத்து வார்த்தைகள் of, in, to

ஆகியவற்றையும், மூன்றெழுத்து வார்த்தைகள் and, the போன்றவற்றையும் சைஃபர் டெக்ஸ்டில் தேடிக் கண்டுபிடிக்க முயலுவர். இப்படி முயற்சி செய்து ப்ளெயின் டெக்ஸ்ட் விபரத்தை அவர்களால் தெரிந்துகொள்ள முடியும். ஏனென்றால் ட்ரான்ஸ்பொசிஷன் சைஃபரில் ப்ளெயின் டெக்ஸ்ட் எழுத்துகள் இடம் மாற்றி எழுதியிருக்குமே தவிர ப்ளெயின் டெக்ஸ்டில் இல்லாத புதிய எழுத்துகள் சைஃபர் டெக்ஸ்டில் இருக்க முடியாது. இதனால் மாற்றுக் குறியீட்டு ஆய்வாளர்கள் முயற்சியால் ப்ளெயின் டெக்ஸ்ட் விவரம் தெரிந்துவிட ஏதுவாகும்.

படம் 3.4 இலுள்ள வார்த்தைகளின் சைஃபர் டெக்ஸ்டு கீழே தரப்பட்டிருக்கிறது.

"LEEHG ANNOA SITPL TNTPO EGOIN VWSNE"

L	A	S	T	E	V
E	N	I	N	G	W
E	N	T	T	O	S
H	O	P	P	I	N
G	A	L	O	N	E

படம் 3.5

L	E	E	H	G	A
N	N	O	A	S	I
T	P	L	T	N	T
P	O	E	G	O	I
N	V	W	S	N	E

படம் 3.6

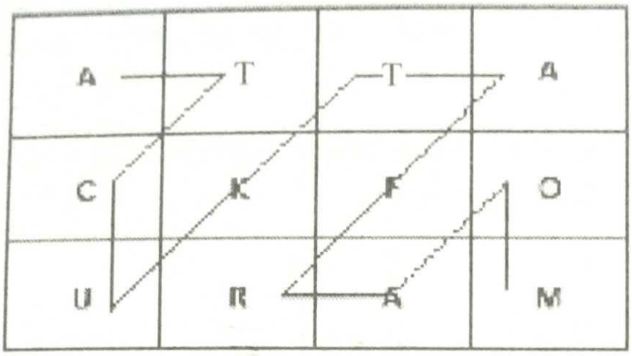
(படம் 3.5 ஐ இன்னொரு முறை மாற்றி எழுதிய encipher)

படம் 3.5 ஐ இரண்டாவது தடவை மாற்றி எழுதிக் கிடைப்பதிலுள்ள சைஃபர் டெக்ஸ்ட் பின்வருமாறு.

"LNTPNENPOVEOLEWHATGSGSNONAITIE"

இந்த சைஃபர் டெக்ஸ்டிலிருந்து ப்ளெயின் டெக்ஸ்ட் என்ன என்பதை தெரிந்து கொள்வது எளிதில்லை.

Plain Text: ATTACK FOUR AM



படம் 3.7 Cipher Text

Cipher Text: ATCUKTAFRAOM

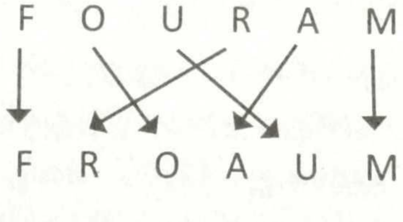
Column, row உள்ள டேபிள் வழி ட்ரான்ஸ் பொஸிஷன் சைஃபர் எழுதுவதற்கு பதிலாக ப்ளெயின் டெக்ஸ்டின் ஒவ்வொரு எழுத்தும் எந்த இடத்துக்கு மாற்றி எழுதப்பட வேண்டும் என்று காட்டுவது மிகவும் வேகமாக செய்யக்கூடிய ஒன்று.

Plain Text: FOURAM

F	O	U
R	A	M

படம் 3.8

Cipher Text: FROAUM



படம் 3.9

மாற்று எழுத்து அட்டவணை (Transportation table) இல்லாமல் FOURAM என்ற ப்ளெயின் டெக்ஸ்டை மறை எழுத்தாக்கியதை படம் 3.9 இல் காட்டப்