खण्ड-7, अंक-1, वर्ष-2019, मु0प्र0 87-91
D.O.I.: 10.22445/avsp.v7i1.16

विश्व युद्धों में साइफर मशीनों का योगदान-एक समीक्षा

प्रीति बाजपेयी
प्रोफेसर, गणित विभाग एवं एसोसिएट डीन स्टूडेन्ट वेलफेअर
बिट्स, पिलानी, दुबई कैम्पस, दुबई, यू0ए0ई0
dr.priti.bajpai@gmail.com

प्राप्त तिथि–30.08.2019, स्वीकृत तिथि–03.10.2019

सार– साइफर मशीनों ने विश्व युद्धों के दौरान बहुत ही प्रमुख भूमिका निभाई और युद्धों को एक नया मोड़ दिया। युद्ध के समय गोपनीय संदेश को सुरक्षित गंतव्य तक पहुंचाना बहुत मुश्किल कार्य था। तत्कालीन जर्मन सेना को इन संदेशों को एन्क्रिप्ट करके भेजने का विचार आया और उन्होंने इसके लिये **एनिग्मा**[1] मशीन का प्रयोग किया। दूसरी ओर पोलैण्ड की सेना को एनिग्मा मशीन की खबर लगी और उन्होंने जब यह सूचना ब्रिटेन के साथ बांटी तो तुरन्त ब्रिटेन ने एक सरकारी 'गवर्नमेंट कोड एण्ड साइफर स्कूल' खोला और एनिग्मा मशीन के द्वारा भेजे गये संदेशों को वे डिक्रिप्ट करने में जुट गये। यह तो सिर्फ एक प्रारम्भ था। समय के साथ अनेक जटिल मशीनें बनी। प्रस्तुत शोध पत्र में इन्हीं प्रमुख मशीनों का इतिहास दिया जा रहा है जो कि विश्व युद्धों में प्रयोग में लायी गयी।

बीज शब्द– साइफर मशीन, एनक्रिप्शन, डिक्रिप्शन, कोड, क्रिप्ट और डिक्रिप्ट

Contribution of Ciphering machines in world wars-a review

Priti Bajpai
Professor, Deptt. of Mathematics and Associate Dean Student Welfare
B.I.T.S. Pilani, Dubai Campus, Dubai, U.A.E.
dr.priti.bajpai@gmail.com

Abstract- Ciphering machines have played a very important role in the conduct of world wars and it was these machines which were responsible for giving the war a new direction. Sending secret messages to the destination without being intercepted was quite crucial and challenging during the war. The need to send crypted messages was first felt by the German army who used the first cipher machine Enigma for this purpose. When British came to know through the polish army about Enigma they opened a Government Code and Cipher School to decrypt the messages sent by Enigma. This was just the beginning. As time progressed more sophisticated machines were made. Present paper embodies a history and role of all the important cipher machines during both the world wars.

Key words- Cipher machine, encryption, decryption, code, crypt, and decrypt

1. **परिचय–** युद्ध के दौरान किसी भी गोपनीय संदेश, सूचना या जानकारी को साइफर से सुरक्षित करके भेजने का प्रचलन जूलियस सीजर के समय से चला आ रहा है। सीजर संदेश के प्रत्येक अंग्रेजी अक्षर को वर्णमाला में उस अक्षर के बाद आने वाले तीसरे अक्षर से बदल देते थे। यह सीजर साइफर के नाम से प्रसिद्ध हुआ। उस समय संदेश को क्रिप्ट और फिर डिक्रिप्ट करना सब हाथ से होता था। परन्तु बीसवीं शताब्दी में विद्युतीय टेलिग्राफी की खोज के बाद साइफर करने के लिये मशीनों का प्रयोग होने लगा। इन मशीनों में बिजली और यांत्रिक पुर्जों का प्रयोग कर संदेश को साइफर कर भेजा जाने लगा। पर संदेश को सुरक्षित पहुँचाना बहुत आवश्यक था। संदेश दुश्मन के हाथ लगने का अंजाम बहुत खतरनाक होता था। सन् 1917 में जर्मनी के विदेश सचिव आर्थर जीमरमैन ने एक संदेश साइफर करके भेजा जिसमें लिखा था कि 'अगर जर्मनी युद्ध जीत गया तो मैक्सिको को उसकी जमीन दिला देंगे'। यह संदेश अंग्रेजों के हाथ लग गया यही वजह थी कि अमरीका विश्व युद्ध में शामिल हुआ। तो यह देखा जा सकता है कि क्रिप्टिड संदेश के पकड़े जाने और डिक्रिप्ट होना कितना खतरनाक था। इस संदेश के पकड़े जाने और डिक्रिप्ट होने से युद्ध को एक नया मोड़ मिला और उसने इतिहास ही बदल दिया।

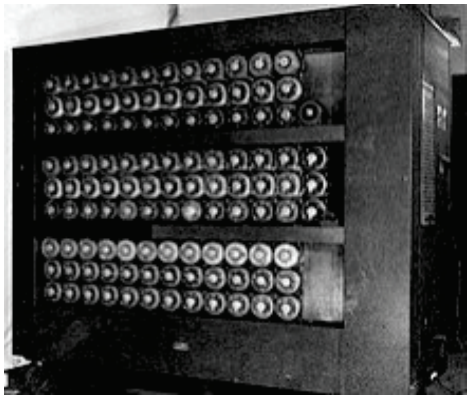
2. **साइफर मशीनों के प्रकार व उनका योगदान–** विश्व युद्धों के दौरान अनेक प्रकार की साइफर मशीनों का प्रयोग हुआ और उनका

बहुत ही महत्वपूर्ण योगदान रहा है। साइफर मशीनों के बारे में अति गोपनीयता रखी गयी है। कोई आश्चर्य की बात नहीं यदि विश्व युद्धों के दौरान प्रयोग होने वाली कुछ मशीनों के बारे में किसी को अभी भी पता न हो। हाल ही में लंदन के सांइस म्यूजियम में एक 'टाप सीक्रेट' नाम से एक प्रदर्शिनी लगी। इसमें विश्व युद्धों में प्रयोग होने वाली साइफर मशीनों को पहली बार दर्शाया गया और एनिग्मा और लौरेंज जैसी मशीनों, जिनके बारे में लोगों ने सिर्फ सुना था, को देखने का मौका मिला।[1]

प्रारम्भ में प्रथम युद्ध के दौरान टेलीफोन पर जरूरी संदेश भेजे जाते थे। यहाँ तक की लड़ाई के मैदान में जो खाई खोदी जाती उसमें भी टेलीफोन के बोर्ड होते पर टेलीफोन पर भेजे गये संदेश बिल्कुल सुरक्षित नहीं होते थे। दुश्मन उन्हें बीच में पकड़ कर सुन सकता था। अंग्रेजों की सौमी युद्ध की योजना को जर्मनी ने फोन पर पकड़ा था और उसी के बाद अंग्रेजी सेना ने फुलर फोन, जो कि कैप्टन एलगरमन फुलर की खोज थी, को प्रयोग करना शुरू किया। इस फोन से मोर्स कोड से संदेश, कम वोल्टेज पर भेजे जाते जिन्हें पकड़ना बहुत मुश्किल था। वैसे तो अंग्रेजी सेना युद्ध के दौरान संदेश भेजने के लिये सिर्फ टेलीफोन का ही इस्तेमाल नहीं कर रही थी। वो जरूरत के हिसाब से अलग–अलग तरीके प्रयोग करती। अंग्रेजी सेना में 30,000 मोटरबाइक सवार थे। इन्हें डिस्पैच राईडर कहा जाता था। अगर संदेश नो मैन्स लैंड पर भेजने होते तो जानवर या पक्षी जैसे कबूतर या फिर घोड़े आदि का प्रयोग होता। मशीनों द्वारा संदेश भेजने का इतिहास जर्मनी से शुरू हुआ।

वर्ष 1923 में एक डच व्यक्ति के सुझाव पर एक जर्मन डॉ0 आर्थर शीबियस ने व्यापार की गतिविधियों को सुरक्षित रखने के लिये एक मशीन बनाई जो बैंको में भी प्रयोग हो सकती थी। तो जर्मन सेना को लगा कि ऐसी मशीन तो युद्ध में संदेश भेजने के लिये भी काम आ सकती है। फिर उन्होंने इसी प्रकार की एक साइफर मशीन बनाई जिसका नाम था एनिग्मा इसमें विद्युत के परिपथ थे और रोटर को घुमा कर संदेश को पूरा बदल दिया जाता। साइफर मशीनों के इतिहास में यह पहली मशीन थी। प्रारम्भ में तो इसमें तीन ही रोटर थे परन्तु बाद में एक रोटर और बढ़ाया गया। जर्मन सेना एनिग्मा के बनने पर मुस्तैदी से संदेश साइफर कर भेजनी लगी और उधर अंग्रेजों को इसका पता भी न था। वो तो सन् 1931 में एक जर्मन जासूस को फ्रेंच लोगों ने पकड़ा जिससे एनिग्मा की जानकारी मिली। फ्रेंच सेना ने यह जानकारी पोलिश सेना को दी। पोलैंड के एक गणितज्ञ मैरियान रेजिविस्की ने एनिग्मा के तार रोटर को कैसे चलाते हैं और रिफ्लैक्टर संदेश कैसे भेजते हैं इसको समझा और गणितीय तरीके से विश्लेषण किया। फिर उन्होंने एनिग्मा जैसी ही एक और मशीन बनाई। यह सब काम बड़े खुफिया तरीके से चल रहा था। सन् 1939 में जब पोलैंड पर जर्मनी के आक्रमण का खतरा हुआ तो उन्होंने वारसौ शहर मे अंग्रेजों के साथ एक बैठक रखी और एनिग्मा की जानकारी उनके साथ बांटी।

एनिग्मा (Enigma)



बौम्बी (Bombe)

इस जानकारी के मिलने से अंग्रेजों ने तुरंत एक गवर्नमेंट कोड एण्ड साइफर स्कूल ब्लेचले पार्क में खोला। पर यह नाम बहुत सांकेतिक था तो बाद में इसका नाम उन्होंने बदल कर गवर्नमेंट कम्यूनिकेशन हेड क्वार्टर रखा। यहाँ उच्चकोटि के गणितज्ञ, कम्प्यूटर के विशेषज्ञ दिन रात एनिग्मा से मिले साइफर संदेशों को डिक्रिप्ट करने मे लग गये। एनिग्मा से मिले संदेशों को वो 'अल्ट्रा' के नाम से बुलाते थे। उधर जर्मन एनिग्मा के साइफर किये संदेशों को ब्रिटिश शैंक के नाम से बुलाते थे। ब्लेचले पार्क में काम इतने खूफिया तरीके से होता था कि कहते हैं कि बहुत समय तक जर्मन सेना को यह पता ही नहीं चला कि अंग्रेजों को एनिग्मा की जानकारी हो चुकी है और वो संदेश पर संदेश भेजते रहे। एनिग्मा से आये संदेश महिला कर्मचारी रेड फॉर्म में लोड करती और ये ब्लेचले पार्क भेजे जाते वहाँ इन्हें डिकोड किया जाता था। ये डिकोडिंग हाथ से होती थी और गणनाओं में बहुत समय लगता था। तब ब्लेचले पार्क ने बौम्बी मशीन बनाई जो गणनायें बहुत तेजी से करती थी। इसी बौम्बी मशीन को एलन टयूरिंग और गौरडन वेलचमन ने स्वचालित किया।[2]

सन् 1936 में एक स्वीडिश व्यापारी बोरिस हैगलिन ने एक मशीन सी–36 बनाई। यह पहली मशीन थी जिसमें लग और पिन(Lug and Pin) डिजाइन का प्रयोग हुआ।[3] यह थी तो एनिग्मा मशीन की ही तरह पर इसमें रोटर और गियर से भी जयादा सैटिंग मिलती। यह मशीन उन्होंने अमरीकी सेना को बेची। आज भी उनकी बनाई कम्पनी स्विटजरलैंड में चल रही है उन्होंने एक और साइफर मशीन एम–209

अमरीकी सेना के लिये बनाई। यह साइफर मशीन टिफिन के डिब्बे के बराबर छोटी थी और उसे इधर–उधर ले जाना आसान था। विश्व युद्ध में अमरीका ने इसका खूब प्रयोग किया।[4]

C-36

M- 209

सन् 1937 में ब्लेचले पार्क में एक और साइफर मशीन टाइपेक्स का प्रयोग प्रारम्भ हुआ जो कि एनिग्मा के आधार पर कार्य करती थी। यह साइफर भी कर सकती थी और एनिग्मा द्वारा भेजे गये संदेशों को डिकोड भी करने में सक्षम थी। जर्मन सेना टाइपेक्स द्वारा भेजे गये संदेशों को कभी भी डिकोड नहीं कर पायी।

सन् 1940 में जर्मनी में जर्मन हाई कमांड, गोपनीय संदेश भेजने के लिये एक मशीन गहिमश्राइबर का प्रयोग कर रही थी। इसमें एक और सुविधा थी कि यह संदेश को डिक्रिप्ट करके उसे प्रिंट भी कर देती थी। ब्लेचले पार्क इससे सम्बन्धित संदेशों को स्टरजन कहते थे। एनिग्मा और लौरेंज के संदेश रेडियो से भेजे जाते पर गहिमश्राइबर के लैंड लाइन से, इसलिये उन्हें डिकोड करना आसान न था।[5]

टाइपेक्स (Typex)

गहिमश्राइबर (Geheimschreiber)

सन् 1940 में ही जर्मन आर्मी ने संदेश भेजने के लिये एक और नई मशीन बनाई जिसका नाम था लौरेंज। इससे भेजे गये साइफर संदेशों की शुरूआत पहले मिलने वाले संदेशों से अलग थी। पहले वाले संदेशों में शुरूआत कैसी है, यह अंग्रेज समझ गये थे। बाद में जर्मन कोडर शुरू में नम्बर डालने लगे। इससे अंग्रेजो को उन्हें डिकोड करना बहुत मुश्किल हो गया। अंग्रेज इन लौरेंज से भेजे गये नये संदेशों को टनी के नाम से बुलाते थे। इसकी भी कहानी बड़ी दिलचस्प है, ब्लेचले पार्क में कोडर विभिन्न संदेशों के नाम मछली के नामों पर रखते थे। तो लौरेंज से आने वाले संदेशो का नाम टूना मछली के नाम से टनी रखा गया और जिस कमरे में लौरेंज से सम्बन्धित काम होता था, उसे अपने प्रमुख रॉल्फ टेस्टर के नाम पर टेस्टरी बुलाते थे। अब जैसे कहा जाता है किसी की गलती दूसरे का फायदा बन जाती है उसी तरह एक जर्मन ऑपरेटर ने लौरेंज से एक ही साइफर संदेश को दो बार भेज दिया। फिर क्या था, ब्लेचले पार्क ने तुरन्त दोनों संदेशों की सेटिंग की तुलना की और संदेश को डिकोड कर लिया और गणनाओं के लिये टनी कैल्क्यूलेटर (Tunny Calculator) का प्रयोग किया। लौरेंज

का प्रयोग या तो हिटलर या उच्च अधिकारी ही करते थे। संदेशों को लड़ाई के मैदान तक भेजने और आपस के विचार विमर्श के लिये ही इसका प्रयोग हो रहा था। लौरेंज से भेजे जाने वाला एक महत्वपूर्ण संदेश कि जर्मन समझ रहे हैं कि हमलावर सैनिक नौरमैंडी में नही उतरेंगे जैसा की पहले प्लान था। अब वे कलाइस के पास उतरेंगे, यह संदेश ब्लेचले पार्क में कोलोसस से डिकोड हुआ। लौरेंज एक उच्च श्रेणी की मशीन थी। इसमें इलेक्ट्रिकल सर्किट से रोटर घूमते और एक–एक करके संदेश के अक्षर को नये अक्षर में बदल देते। संदेश भेजने वाले और पाने वालों को प्रारम्भ की सेटिंग पता होती और इस बारे में पूरी गोपनीयता रखी जाती। असली संदेश को भेजने के पहले बारह अक्षरों को बिना बदले भेजा जाता। उधर रिसीवर प्रत्येक शब्द के पहले अक्षर को ग्रिल पर पढ़कर रोटर की सेटिंग का पता लगा लेता।[6]

लौरेंज (Lorenz)

कोलोसस (Colossus)

सन् 1941 में जर्मनी ने एक और महत्वपूर्ण मशीन एसजी–41 बनाई। इसे हिटलर मिल के नाम से जाना गया। इसका प्रयोग जर्मन खुफिया एजेंसी अबवेहर ही करती थी और वो भी बहुत कम। यह मशीन टाईपरायटर बनाने वाले एक व्यक्ति वानडरर और फ्रिट्स मेनजर ने बनाई थी। यह भी सी–36 मशीन की ही तरह थी परन्तु बहुत भारी थी जिसकी वजह से युद्ध के मैदान में नहीं ले जाई जा सकती थी। पर यह इतनी शक्तिशाली मशीन थी कि इसके द्वारा भेजे गये संदेश को ब्लेचले पार्क कभी नही तोड़ पाया।[7]

साइको (SYKO)

SG-41

सन् 1943 में पोस्ट ऑफिस के एक इंजीनियर टौमी फ्लॉवर ने सुझाव दिया कि एक मशीन जो कि पूरी तरह इलेक्ट्रॉनिक हो, अगर बनाई जाये तो लौरेंज द्वारा भेजे गये संदेशों की सेटिंग आसानी से पता लगायी जा सकती है। इस मशीन में उनका सुझाव था कि काँच के रेडियो वॉल्व लगाये जायें पर लोग उनसे सहमत नहीं थे, उनका सोचना था कि, ये वॉल्व चले न चले तो इस मशीन के बनने का शुरू में बड़ा ही विरोध हुआ। इसका नाम था कोलोसस और यह सन् 1944 में बनकर तैयार हुई। ऐसी सिर्फ 10 मशीनें बनी और इनके बारे में युद्ध के बाद भी गोपनीयता रखी गई। कहते हैं दो मशीनों को छोड़कर बाकी सब को खोल डाला गया और उनके पुर्जे प्रयोग कर लिये गये। सन् 1950

में दो में से एक मशीन का प्रयोग तो हुआ पर कहाँ और क्यों ये कोई भी नही जानता।[8–10]

सन् 1943 में ब्रिटिश आर्मी एक और मशीन का इस्तेमाल कर रही थी जिसका नाम था साइको (SYKO) पर ज्यादातर रॉयल एअर फोर्स ही हवाई जहाज में जमीन पर संदेश भेजने के लिये करती थी, पर ये संदेश सुरक्षित नहीं रहते थे। सन् 1944 में जर्मन सेना एक और मशीन रैश्टरश्लुसल–44 साइफर मशीन का प्रयोग कर रही थी। इसके द्वारा साइफर किये संदेश डिकोड करना बहुत ही मुश्किल था। उसमें असली संदेश को कुछ रो में लिखते और कुछ कॉलम छाँट कर डिक्रिप्ट करते। प्रयुक्त 'की' में रो और कॉलम की जानकारी दी होती थी।[11]

निष्कर्ष– बहुत से लोगों का मानना है कि ब्लेचले पार्क में इन जर्मन मशीनों, एनिग्मा और लौरेंज के कोड को तोड़ पाने के कारण से ही ब्रिटेन और संयुक्त सेनाओं (एलाइड फोर्सेज) की विश्व युद्ध में विजय हुई और युद्ध शीघ्र खत्म हुआ। युद्ध के समाप्त होने से लाखों लोगों की जानें बचीं। विन्स्टन चर्चिल ने कहा है कि एलन ट्यूरिंग का सबसे बड़ा योगदान एलाइड फोर्सेज की जीत में रहा है।[12]

संदर्भ

1. https://en.wikipedia.org/wiki/Enigma_machine#/media/File:EnigmaMachineLabeled.jpg
2. https://en.wikipedia.org/wiki/Bombe
3. https://en.wikipedia.org/wiki/C-36_(cipher_machine)
4. https://en.wikipedia.org/wiki/M-209
5. https://en.wikipedia.org/wiki/Typex#/media/File:Typex_nocase.jpg
6. https://en.wikipedia.org/wiki/Siemens_and_Halske_T52
7. https://www.cryptomuseum.com/crypto/lorenz/sz40/index.htm
8. https://en.wikipedia.org/wiki/Colossus_computer
9. https://www.cryptomuseum.com/crypto/sg41/index.htm
10. https://upload.wikimedia.org/wikipedia/commons/6/65/SYKO-SD_2_Strip_Cipher%2C_1950s_
11. National_Cryptologic_Museum_-_DSC07999.JPG
12. http://users.telenet.be/d.rijmenants/en/rasterschlussel44.htm