Die Kryptographie

Autor(en): **[s.n.]**

Objekttyp: **Article**

Zeitschrift: **Pionier : Zeitschrift für die Übermittlungstruppen**

Band (Jahr): **34 (1961)**

Heft 6

PDF erstellt am: **16.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-562690

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

kehrt. Dennoch müssen die Angehörigen der Übermittlungstruppen und der Übermittlungsdienste nach einheitlichen Gesichtspunkten und Vorschriften ausgebildet werden. Eine solche Ausbildung ist besonders dort unumgänglich, wo Übermittler verschiedener Waffen mit ihren Truppen zu gemeinsamem Einsatz gelangen. Das wird immer die Regel sein bei der Zusammenarbeit zwischen Infanterie und Panzer oder zwischen Infanterie und Artillerie (Unterstützungsfeuer). Doch auch die Funker der Übermittlungstruppen und der Übermittlungsdienste haben gemeinsame Berührungspunkte: im sogenannten Führungsnetz. In ein solches Führungsnetz eingeschlossen sind die Funkstationen der Divisions- und Brigadekommandos und die Stationen der diesen direkt unterstellten Truppenkörper der Infanterie, der Leichten Truppen und der Artillerie. Dieses Führungsnetz benützen die Kampftruppenkommandanten für direkte Befehle an die Divisions- und Brigadekommandanten. Einheitlichkeit der Verkehrsregeln, der Tarnung der Übermittlung und der Identifizierung der Stationen sind unbedingt notwendig. Disziplin und rasche Übermittlung spielen gerade im Führungsnetz eine entscheidende Rolle, so dass es unumgänglich ist, dass die Soldaten, denen der Betrieb des Führungsnetzes vorbehalten ist, zeitweise zusammengefasst und gemeinsam ausgebildet werden.

Die Kryptographie

In der Absicht, ihren Gegnern oder ihren Rivalen die eigenen Pläne zu verheimlichen, haben zu allen Zeiten Fürsten, Verschwörer, Bankleute, Gefangene und Soldaten geheime Schriften verwendet. Die Geheimhaltung von Meldungen geschieht bisweilen durch das Verstecken derselben, durch die Verwendung besonderer Tinten, durch das Einflechten vereinbarter Zeichen in harmlos scheinenden Darstellungen usw.

Diese Verfahren bieten allerdings nur eine beschränkte Sicherheit, und der Erfolg ist eher schwach. Aus diesem Grunde wird manchmal verzichtet, den geheimen Charakter eines Dokuments zu verbergen, indem es in eine sichtbar verworrene Reihenfolge von Ziffern oder Buchstaben, nach einer mit dem Empfänger getroffenen Vereinbarung, umgewandelt wird.

Ein solches Kryptogramm oder chiffrierte Meldung kann nach freier Wahl befördert werden: durch die Post oder, nach vorgenommener Einteilung in Gruppen zu 5 Zeichen, durch Telegraph oder Funk. Bei der Ankunft wird die Meldung in umgekehrter Richtung vom Empfänger behandelt, d. h. dechiffriert. Die Dechiffrierung ist ein mechanischer Vorgang, der methodisch vorgenommen werden muss. Eine chiffrierte Meldung verrät aber eine bestimmte Bedeutung, und der Feind wird keine Mühe scheuen, deren Sinn herauszufinden. Die Operation ist aber für ihn wesentlich schwieriger, da er sowohl den klaren Text, wie auch den vereinbarten Schlüssel erraten muss. Das ist die Arbeit ausgesuchter Spezialisten, Dekrypteure genannt.

Die Geschichte der Kryptographie entspricht einem langjährigen, aber noch nicht abgeschlossenen Wettkampf zwischen Chiffreuren und Dekrypteuren. Daraus ergaben sich schon lustige, aber auch tragische Anekdoten. Chiffreure und Dekrypteure haben abwechselnd grossartige Erfolge geerntet und ihre wunderbaren Resultate haben öfters Schriftsteller und besonders Autoren von Kriminalromanen inspiriert. Auch Erfinder haben mit mehr Selbstvertrauen als Sachkenntnis das Problem der Chiffrierung angepackt und glaubten «neue» und «unantastbare» Verfahren entdeckt zu haben, die aber vom Kryptologen augenblicklich zu den elementarsten, bekannten Methoden zurückversetzt wurden.

Chiffrierverfahren bestehen in praktisch unbeschränkter Anzahl. Sie können aber alle in bestimmte Klassen eingereiht werden, für welche der Dekrypteur passende Dekryptierverfahren kennt.

Es kann aber festgestellt werden, dass selbst unter Verwendung der vollkommensten Maschinen weder ein absolut sicheres Chriffrierverfahren noch ein unfehlbares Dekryptierungssystem erfunden wurden!

Die elementaren Chiffrierverfahren

Zur Chiffrierung werden zwei grundsätzliche Operationen angewendet, die einzeln oder kombiniert zur Anwendung kommen können:

— Die *Transposition* besteht im Wechseln der Elementanordnung, wie z. B. die Umstellung der Buchstaben eines klaren Textes in eine scheinbar sinnlose Reihenfolge.

— Die *Substitution* besteht im Ersatz der Elemente des Textes — Buchstaben, Wörter oder Silben — durch andere Elemente, bestehend aus Buchstaben, Wörtern, Zahlen oder anderen beliebigen Zeichen, die aus Listen (Codes oder Wörterbüchern) entnommen oder nach besonderen Regeln zusammengestellt wurden.

Die Scytale der Griechen ist eines der ältesten Chiffrierverfahren. Es bestand aus einem Holzlineal, um welches das Schriftband umgewickelt war, also einer äusserst primitiven Chiffriermaschine. Die Meldung wurde auf das aufgerollte Band geschrieben, und das abgewickelte Band war mit einem Text versehen, dessen Buchstaben umgestellt waren. Es war nun für den Empfänger leicht, das Band wieder gleich zu wickeln — er musste dafür ein gleichgeformtes Lineal wie der Absender verwenden —, um den Text zu lesen. Der heutige Dekrypteur würde, um den vorgelegten Text zu lesen, sich begnügen, immer die gleiche Zahl von Buchstaben zu überspringen oder den Text in Gruppen von zwei, drei, vier Buchstaben abzuschreiben in rechteckige Tabellen, worin der Klartext schliesslich in den Kolonnen erscheint.

Julius Cäsar wendete die einfachste Methode der Substitution an: sie bestand darin, jeden Buchstaben zu ersetzen durch denjenigen Buchstaben, der durch eine gleichbleibende Verschiebung im normalen Alphabet erhalten wird, z. B. A durch K, B durch L, C durch M, usw. Zur Vereinfachung der Chiffrierung und der Dechiffrierung kann ein dem Rechenschieber ähnliches System angewendet werden, d. h. 2 nebeneinander liegende Schieber mit einem mehrfach aufgeführten Alphabet, damit eine teilweise Überdeckung ermöglicht wird. Beim Wechsel der Verschiebung wird der Schieber versetzt bis zum Übereinstimmen der Buchstaben des Klartextes und des Kryptogrammes. Der mit dem Substitutionsalphabet versehene Schieber kann auch mit einem Alphabet in rückwärts laufender oder sogar willkürlicher Reihenfolge versehen werden.

Wie dekryptieren?

Wenn wir bis in die Zeit vor der Renaissance zurückgehen, da die Kryptoverfahren noch ziemlich rudimentär waren, kann angenommen werden, dass der damalige Dekrypteur sich bei der Bearbeitung eines Textes fragen musste, ob der Text nach dem beschriebenen einfachen Transpositionsverfahren oder nach der Methode Julius Cäsars chiffriert wurde. Trotz der anscheinenden Zusammenhangslosigkeit weisen beide Systeme Eigenschaften auf, die den Dekrypteuren helfen, auf die richtige Spur zu kommen. Bei den einfachen Substitutionsmethoden bleiben die Buchstaben an ihren normalen Plätzen und werden immer durch dieselben Buchstaben ersetzt. Wenn angenommen wird, dass der Text in französischer Sprache vorliegt, werden alle Buchstaben nicht mehr in gleicher Häufigkeit erscheinen. Der Buchstabe «E» erscheint am häufigsten (durchschnittlich 14%), dann folgen in abnehmender Häufigkeit die Buchstaben S, A, R, T, I, N, L, O, C, wobei die Reihenfolge der vier letztgenannten Buchstaben von verschiedenen Kryptologen anders angegeben wird. Wenn also in einem nach Cäsars Methode chiffrierten Text ein Buchstabe in einer Häufigkeit von ca. 14% erscheint, kann wohl angenommen werden, dass es sich um ein «E» handelt. Ebenso verhält es sich mit den Bigrammen (Buchstabenpaare). «ES» wird am häufigsten angetroffen (3%), dann folgen LE (2,4%) und EN (2,4%). Es wird somit nach den Bigrammen gesucht, die häufig vorkommen und die eines der erwähnten Bigramme darstellen können. Somit kann geprüft werden, ob die Substitution des «E» richtig ist. Es folgen dann die Doppelbuchstaben, in ihrer abnehmenden Häufigkeit «SS, LL, TT und MM». Das «Q» ist fast immer von einem «U» gefolgt. Diese Bemerkungen geben eine Ahnung über die Art des verwendeten Substitutionsverfahrens und mit dem Erraten weiterer Buchstaben und Erkennen von Wörtern kann das Substitutionsalphabet zusammengestellt werden.

Wurde eine Transposition des Textes angewendet, gehen die Bigramme auseinander; die Buchstaben bleiben hingegen unverändert; das «E» wird somit immer am häufigsten angetroffen, dann folgen S, A, R usw. Damit erkennen wir, dass es sich um eine Transposition handelt; abzutasten bleibt, nach welchen Prinzipien diese erfolgte.

Wurde der Text in zwei Stufen chiffriert, durch Transposition, dann durch Substitution, so hat man es mit einer Überchiffrierung zu tun. Das Dekryptieren ist in diesem Augenblick schwieriger, doch gibt es der Dekrypteur noch nicht auf: er wird feststellen, dass das Häufigkeitsgesetz durch diesen doppelten Arbeitsgang keine Änderung erfahren hat. Er verfügt bereits über eine Fährte.

Bei diesem ersten Beispiel der Überchiffrierung können wir feststellen, dass eine solche erst dann eine Verbesserung liefert, wenn beide angewandten Chiffrierverfahren grundverschieden sind: wenn z. B. zweimal nacheinander eine Chiffrierung nach dem Cäsar-Verfahren vorgenommen wird, erhalten wir schliesslich einen Text mit einer Verschiebung entsprechend der Summe der vorgenommenen Verschiebungen; die Dekryptierung ist somit nicht schwieriger geworden.

Das System von Vigenère

Als die vorerwähnten Methoden bekannt wurden, drängten sich andere Verfahren auf. Die Bemühungen gingen dahin, die wesentlichen Bigramme und Trigramme des Textes sowie die Häufigkeiten zu verschleiern. Ein relativer Erfolg zeigte sich in der sinnreich ausgedachten Anwendung von wechselnden Verschiebungen der Substitutionsalphabete.

So hatte sich im 17. Jahrhundert der Belgier Gronsfeld vorgenommen, jeweils jeden Buchstaben des Klartextes nach einem wechselbaren, vorbereiteten Zahlenschlüssel zu verschieben und nicht mehr um eine konstante Anzahl wie bei der Methode Cäsars.

Als Beispiel sei der Schlüssel 21456 angenommen. Der Klartext wird in Gruppen zu 5 Buchstaben aufgeteilt. In jeder Gruppe wird der erste Buchstabe um 2, der zweite um 1, der dritte um 4, der vierte um 5, der fünfte um 6 Ränge verschoben.

Man stellt dabei fest, dass die im Klartext wiederholten Buchstaben (Buchstabenpaare) im chiffrierten Text verschwinden. Ebenso sind Buchstaben mit charakteristischen Häufigkeiten nicht mehr anzutreffen.

Wenn auch das System Gronsfelds 50 Jahre nach demjenigen von Blaise de Vigenère bekannt wurde, so weist Gronsfelds Methode doch keine wesentliche Neuerung gegenüber Vigenère auf; sein System ist sogar in der Anwendung weniger bequem.

Vigenère schuf eine Buchstabentabelle von 26 Zeilen gemäss

```
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 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 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 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
- - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - -
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
```

Zur Chiffrierung eines Textes wählte er einen Schlüssel, bestehend aus einem mehr oder weniger langen Wort oder aus mehreren Wörtern. Die Meldung wird unter den Schlüssel geschrieben; den Buchstaben des Kryptogramms findet man im Schnittpunkt der mit dem Schlüsselbuchstaben beginnenden Kolonne und der mit dem Klartextbuchstaben beginnenden Zeile; z. B. ergibt der Klarbuchstabe «D», chiffriert mit dem Schlüsselbuchstaben «T» den Chiffrebuchstaben «W».

Das zum Verfahren von Gronsfeld angegebene Beispiel lässt sich ebenfalls erhalten nach dem System von Vigenère mit dem Buchstabenschlüssel CBEFG, welcher allerdings, weil sinnlos, nicht leicht im Gedächtnis behalten werden kann.

Das am Schluss des 16. Jahrhunderts erfundene System konnte bis Mitte des 19. Jahrhunderts den Anstrengungen der Dekrypteure standhalten. Zweckmässig angewandt, mit einem relativ langen Schlüssel zu kurzen Texten, bietet es eine gewisse Sicherheit. Es ist gleichwohl gelungen, ein System der Dekryptierung auszuarbeiten auf folgender Grundlage: Beim Chiffrieren wird der Klartext, entsprechend der Länge des Schlüssels, in Abschnitte eingeteilt. Schreibt man diese Abschnitte untereinander, so werden die Buchstaben derselben Kolonne mit demselben Schlüsselbuchstaben chiffriert. Demzufolge, wenn gewisse Buchstabenpaare, Bigramme oder Trigramme im Schema untereinander figurieren, ergeben sich gleichlautende Buchstabengruppen im chiffrierten Text. Wenn solche Wiederholungen in einem Kryptogramm beobachtet werden, sind sie nicht einem Zufall zuzuschreiben und können einen wertvollen Hinweis geben für die Länge des Schlüssels: In der Tat, wenn sich die betreffenden Buchstabengruppen untereinander auf der Tabelle befinden, ist ihre Distanz ein Vielfaches der Schlüssellänge. Der Dekrypteur notiert all diese Wiederholungen und stellt als Schlussfolgerung die Länge des Schlüssels fest.

Er kann dann die chiffrierte Meldung auf ebenso viele Kolonnen abschreiben und weiss, dass jede einzelne Kolonne

mit dem gleichen Buchstabenschlüssel chiffriert wurde. Hier macht sich wieder das Gesetz der Häufigkeit bemerkbar, und es ist höchstwahrscheinlich, dass der am häufigsten auftretende Buchstabe als «E» zu betrachten ist. Durch diese Häufigkeitserscheinungen wird somit versucht, den Buchstabenschlüssel zu erraten, und bald wird es möglich sein, den ganzen Text zu dekryptieren.

Es kann sein, dass der Schlüssel lang und die Meldung daher schwierig zu dekryptieren ist. Wenn hingegen mehrere Meldungen vorhanden sind und angenommen werden kann, dass sie mit dem gleichen Schlüssel chiffriert worden sind, dann können wertvolle Hinweise daraus gezogen werden, z. B. dass die gleichrangigen Buchstaben mit dem gleichen Schlüssel chiffriert wurden.

In der Praxis heisst es tatsächlich, einen chiffrierten Text nie allein zu betrachten, sondern alle möglichen Unterlagen beizuziehen und zu vergleichen. Insbesondere kann es vorkommen, dass bestimmt angenommen werden kann, dass das Chiffrat das Wort «Schlacht» enthält. In diesem Falle wird das Wort dem Kryptogramm entlang verglichen und festgestellt, welche möglichen Schlüssel die Chiffrierung dieses Wortes an der betreffenden Stelle gestatten: diese Methode des «mot probable» ist in der Kryptologie üblich und leistet grosse Dienste.

Autoklave Verfahren

Zur Erschwerung der Aufgabe des Dekrypteurs wurde versucht, unbegrenzte Schlüssel zu bilden. Eine anscheinend leichte Lösung bestand dahin, sich der Exemplare eines gleichen Buches zu bedienen und zu vereinbaren, ab welchem Punkt der Schlüssel zu verwenden ist. Dieses System ist allerdings im Felddienst unbrauchbar. Man ging deshalb dazu über, entweder den klaren Text oder das Kryptogramm zur Schlüsselbildung zu verwenden; das ist die autoklave Methode.

Die durch diese Methode erwartete Sicherheit ist aber meist illusorisch. Wenn das Kryptogramm als Grundlage zur Chiffrierung diente, kann dieses gegenüber sich selbst verschoben werden; nach einigen Versuchen taucht der Schlüssel plötzlich auf. Wurde die Meldung mit dem Klartext chiffriert, ist daran zu denken, dass die haufigsten Buchstaben «E» und «S» sind und dass durch ihre Begegnung «W» im Kryptogramm entsteht. Die Zwischenräume zwischen zwei gleichen Buchstaben werden notiert und der häufigste Zwischenraum entspricht der Länge des Schlüssels, welcher nach einigen Versuchen erraten wird.

Die Transpositionen durch Raster und Gitter

Wir wollen durch dieses knappe Exposé nicht den Anspruch erheben, sämtliche Chiffrierverfahren und sämtliche Dekryptierungsmethoden analysiert zu haben. Es sei nur erwähnt, dass die Transpositionsverfahren, dank der Verwendung von Schlüsseln, ins Unendliche ausgedehnt werden können.

Nehmen wir als Beispiel einen Schlüssel zu 5 Buchstaben «MARNE» und numerieren darin die Buchstaben nach ihrer normalen Reihenfolge im Alphabet: 31542; dann teilt man den Text in eine rechteckige Tabelle zu fünf Kolonnen auf. Anschliessend werden die Buchstaben, nicht mehr in ihrer Reihenfolge 31542, sondern kolonnenweise in der Reihenfolge 12345 aufgenommen. Der Dekrypteur schreibt den Text auf verschiedene Streifen, die er systematisch gegeneinander verschiebt, bis er klare Textstücke entdecken kann. Die Methode des «mot probable» wird ihm auch in diesem Falle grosse Dienste leisten.

Die Gitter bestehen aus durchbrochenen Papierblättern, die eine Karierung zudecken. Der Text wird in die Fenster des Gitters geschrieben und die Karierung wird durch beliebige Buchstaben ergänzt. In andern Fällen wird das Gitter zur Verwendung neuer Fenster gedreht. Der wesentliche Nachteil der Gitter besteht in ihrer Verbreitung; nie kann man sicher sein, ob der Feind nicht auch Exemplare oder Kopien davon besitzt.

Die Codes

Will man einen Code in Form einer Tabelle zusammenstellen, so werden die darzustellenden Buchstaben, Silben, Wörter, Interpunktionszeichen und Zahlen in die verschiedenen Felder der Tabelle eingeordnet, deren Linien und Kolonnen numeriert sind. Jedes Element ist dann durch den Rang der Linie und den Rang der Kolonne, wo es sich befindet, dargestellt.

Ein Wort kann sich ganz in einem Felde befinden, kann aber auch Silbe für Silbe, sogar Buchstabe für Buchstabe dargestellt werden. Das hat eine ziemlich grosse Auswahl von Darstellungen des gleichen Textes zur Folge, vorausgesetzt, dass der Chiffreur sich dazu bemüht!

Will man die zu chiffrierenden Elemente leicht finden, so müssen sie methodisch geordnet werden: Zahlen zusammen, Interpunktionszeichen zusammen, usw. Aber durch diese Notwendigkeit, verbunden mit einer möglichen Nachlässigkeit des Chiffreurs oder des Redaktors der Meldung (z. B. Meldungen, die immer gleich beginnen: An den Kommandanten der . . .) wird es dem Dekrypteur leicht sein, das Prinzip der Klassifikation zu finden, die er zur Bildung des Sachverzeichnisses benötigt.

Die Chiffrier- und Dechiffriermaschinen

Nach kurzer Überlegung kann festgestellt werden, dass eine grosse Zahl der beschriebenen Systeme, insbesondere das System von Vignère, intellektuelle Handlungen bedingen, die gleich wie Addition und Multiplikation sich durch Rechenmaschinen mechanisieren lassen. Es wurden zahlreiche und raffinierte Chiffriermaschinen erfunden, die von einem in Klartext auf der Tastatur geschriebenen Text die Erzeugung von einem bis zwei Kryptogrammen ermöglichen. Sie erlauben eine rasche und fehlerfreie Chiffrierung und die Anwendung einer praktisch unbegrenzten Anzahl von Schlüsseln. Vor dem Kriege hatte Belin eine interessante Maschine erfunden: Es handelte sich darum, die normale Übermittlung von Bildern zu verschleiern, indem die Rotationsgeschwindigkeit und die Funktionsweise gewisser Organe des Belinographes — Apparat zur Übertragung von Bildern — verändert wurde. Das Resultat bestand aus einer sinnlosen Zusammensetzung von Punkten auf dem Empfänger, die aber, auf einem richtig eingestellten Empfänger, das Bild richtig wiedergaben.

Ein Kampf, der nie aufhören wird

Am Schlusse dieser summarischen Studie werfen wir noch einen Blick auf eine dem Dekrypteur zur Verfügung stehende Waffe zur Meisterung seiner Aufgabe. Im allgemeinen kennt er sämtliche Verfahren, welche bis zu einer bestimmten Zeit erfunden wurden; er bringt es sogar fertig, voraussehen zu können,welche Systeme in einem bestimmten Falle angewendet wurden. Er kennt unter Umständen Absender und Empfänger und ahnt den Inhalt der Meldung. Er kann sogar mit der Ungeschicklichkeit des Feindes rechnen: Hat sich ein Irrtum eingeschlichen, wird die Meldung

wiederholt. Gewisse naive Chiffreure handeln so nachlässig, dass sie unverstandene Worte im Klaren durchgeben; das war seinerzeit die grosse Unvorsichtigkeit Napoleons, die zur Folge hatte, dass alle seine Meldungen vom Feinde dekryptiert wurden. Die Art und Weise wie ein Chiffrierverfahren angewendet wird, erhöht oder vermindert die Sicherheit desselben: ein stereotyp arbeitender, phantasieloser Chiffreur liefert dem Dekrypteur unwillkürlich bedeutend mehr Merkmale, als derjenige, der seine Spezialität beherrscht.

Schliesslich darf die Chiffrierung erst nach reiflicher Überlegung zur Anwendung gelangen; der Zeitbedarf und die Gefahr, den Arbeitsgang zu überladen, sprechen in vielen Fällen für die offene Sprache, insbesondere bei unsteter Lage und wenn der Inhalt einer Meldung sofort ausgewertet werden muss. Mit den Fortschritten der Elektrotechnik ist der Funk nicht mehr nur als Übermittlungsmittel zu betrachten. Die Impulsmodulation der Ultrakurzwellen verlangt ohnehin zwischen Sender und Empfänger eine Verständigung, die, ohne ausdrückliche Vereinbarung zwischen den Korrespondenten nicht realisierbar wäre.

Die Wahrung der Geheimhaltung verschiebt sich allmählich in die Übermittlungstechnik und es werden Übertragungsverfahren angestrebt, die eine Verständigung im Klartext ermöglichen, ohne dass ein Eindringen des Mithörenden befürchtet werden muss.

La modulation de fréquence et sa technique

Pour le technicien, la modulation de fréquence ne se limite pas à la radiodiffusion, c'est un procédé de modulation qui trouve des applications dans de nombreux autres domaines. Aussi nous paraît-il nécessaire d'en bien connaître les bases physiques, avant de passer à la technique pour finir aux réalisations; le sujet n'est pas si aride qu'un petit effort d'assimilation n'en triomphe.

Porteuse et modulation

Nous savons qu'un conducteur parcouru par un courant électrique continu engendre dans l'espace environnant un champ magnétique. Pour s'établir, ce champ emprunte de l'énergie au circuit, énergie qu'il lui restitue au moment de la rupture du courant: c'est le phénomène d'auto-induction ou self-induction.

Si c'est un courant alternatif qui parcourt le conducteur, le champ magnétique engendré est aussi alternatif à la fréquence du courant. Il se propage dans l'espace à la vitesse de la lumière en soustrayant continuellement de l'énergie au circuit. On dit que ce circuit rayonne de l'énergie électromagnétique; cela est vrai pour tous les circuits. Mais la quantité d'énergie rayonnée est essentiellement fonction des dimensions du circuit par rapport à la *longueur d'onde* du courant alternatif qui le traverse.

La longueur d'onde est liée à la *fréquence* du courant par la relation connue: $\lambda = \frac{v}{f}$ ou en mètres: $\lambda = \frac{3 \cdot 10^8}{f \cdot c/s}$.

Ceci explique qu'une ligne de transport d'énergie électrique à 50 c/s, fréquence correspondant à $\lambda = \frac{3 \cdot 10^8}{50} = 6 \cdot 10^6 = 6000$ km, perd, par rayonnement, une quantité d'énergie infime quoique parcourue par des courants énormes, alors qu'à 100 Mc/s, par exemple ($\lambda = 3$ m), deux tiges de cuivre de 0,75 m peuvent rayonner des kilowatts.

Nous savons d'autre part que le phénomène réciproque du rayonnement électromagnétique existe. Il se traduit par le fait qu'un conducteur placé dans un champ électromagnétique est le siège d'un courant induit à la fréquence même du champ. Savoir mettre en évidence et utiliser ce courant induit, c'est être à même de réaliser une liaison radioélectrique.

Le champ électromagnétique est donc le «véhicule» assurant la liaison, l'onde correspondante est dite *onde porteuse*. Le message à transmettre constitue en quelque sorte la «charge utile» dont on veut lester la porteuse, la modulation étant l'art d'incorporer cette «charge» à la porteuse.

— Il est évident que le seul fait de la présence ou de l'absence de la porteuse au lieu de réception peut déjà avoir une signification. Il suffira de coder ces «présences» et ces «absences» de porteuse, le morse n'est pas autre chose, pour transmettre un message complet; c'est ainsi que furent obtenues les premières liaisons radiotélégraphiques. C'était une modulation par «tout ou rien», procédé par trop rudimentaire pour satisfaire longtemps les techniciens de l'époque. Aussi allait-on faire appel rapidement à des formes de modulations plus nuancées qui permettraient de transmettre la parole et les sons, puis les images.

Du point de vue physique, moduler une onde, c'est asservir une ou plusieurs de ses grandeurs caractéristiques au signal à transmettre. Voyons donc quels sont ces éléments caractéristiques, les procédés de modulation possibles en découlent immédiatement.

— Le courant alternatif à haute fréquence constituant l'onde porteuse est représenté graphiquement figure 1. On voit que le courant est tantôt positif, tantôt négatif, sa valeur *i* à un intant *t* quelconque est donnée par la relation:

$$i = a \sin \omega t + \varphi_0.$$

Dans cette expression, le terme *a* est l'*amplitude* de l'onde, soit 10 A, par exemple; le terme ω est la *pulsation* liée à la *fréquence* par la relation: $\omega = 2 \pi f$; à 100 Mc/s, $\omega = 2 \pi \cdot 10^8$; enfin φ_0 est la *phase* à l'origine, soit 90° sur la figure 1. Suivant que la modulation affectera le terme *a*, ω, ou $(\omega t + \varphi_0)$, on aura opéré une modulation d'amplitude, de fréquence ou de phase.

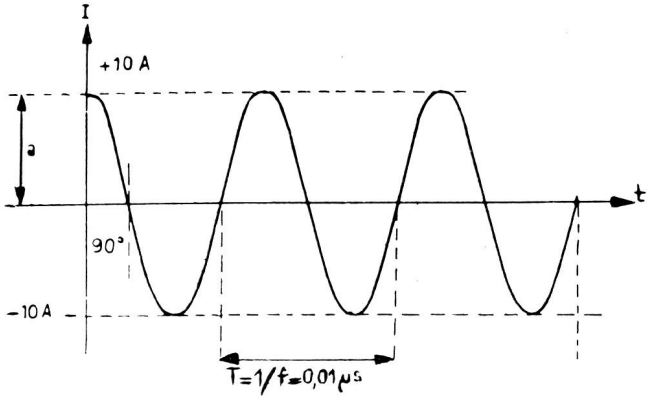

Fig. 1. L'onde HF et les grandeurs qui la caractérisent.