CRIPTOGRAFIA

(Pontos organizados pelo Ministério das Relações Exteriores)

DEFINIÇÃO — OBJETO

ENTRE os meios de transmissão para o estabelecimento de comunicações ocupa o lugar de maior destaque o telégrafo, com ou sem fio Ambos permitem, porém, a intercepção dos despachos, fato que em relação à radiotelegrafia é extremamente notável, dada a facilidade com que são interceptados os despachos transmitidos por êsse meio; como, porém, o seu emprêgo é de grande e cada vez maior utilidade, quer na guerra, quer na paz, impôs-se a necessidade de transformar o texto dos despachos de modo a não poderem ser entendidos pelo adversário ou terceiros, ou seja, a obrigação de substituí-lo por um texto secreto redigido de forma a representar, convencionalmente, o documento original, só podendo ser entendido pelos que conhecerem a convenção que serviu para redigí-lo. Encarando, pois, o problema da criptografia, de um ponto de vista geral, consiste êle em: *a*) dado um texto claro, transformá-lo em outro redigido de modo que só possa ser entendido por quem conheça a significação dos seus elementos; *b*) dado um texto assim transformado, traduzí-lo no texto ou linguagem claros que lhe deram origem.

A organização de um texto secreto pode ser incluída em um dos quatro tipos seguintes: 1.º) grafia invisível; 2.º) grafia dissimulada; 3.º) grafia convencional; 4.º) grafia cifrada. O primeiro é empregado exclusivamente na correspondência e obtém-se com o uso de uma tinta que não se distingue em um exame superficial, mas que se revela por meio de um agente de origem física, como a luz, o calor, ou por um líquido no qual a imersão do texto provoca uma reação química, revelando-o. O segundo consiste em um texto normal, isto é, em um texto que tem um sentido aparente apreciável à primeira vista, onde são hàbilmente dissimulados os elementos que constituem o texto secreto a transmitir. O terceiro, grafia convencional, assim especialmente chamada, consiste no emprêgo de uma redação com tôda a aparência de normal, apresentando um sentido aparente perfeito, mas onde os vocábulos têm, de fato, uma significação diferente e convencional. Não chamando a atenção sôbre o seu verdadeiro objetivo, essa circunstância faz com que êsse processo seja o preferido pelos espiões, conspiradores, etc. O quarto, ou seja, a grafia cifrada, é a mais completa e é aquela em que os documentos são redigidos de uma forma convencional, mas não apresentam o aspecto de uma linguagem normal, mostrando, à primeira vista, que se trata de um texto transformado com o fim de não ser entendido senão por quem conheça a convenção que serviu para organizá-lo. Os documentos assim redigidos constituem o que se denomina *criptogramas* pròpriamente ditos. Um criptograma pode ser redigido por meio de caracteres da grafia usual, sejam algarismos, sejam letras do alfabeto. Êstes são usados quase que exclusivamente pelo Exército, Marinha e diplomacia e, em tempo de paz, pelos grandes estabelecimentos bancários, pois constituem a linguagem secreta mais segura, mais completa e mais prática.

Assim, pois, a arte que preside aos trabalhos de cifração dos textos claros denomina-se *criptografia*.

ORIGEM E EVOLUÇÃO

A necessidade de uma linguagem secreta deve ser tão antiga quanto o homem e pode-se afirmar que a arte correspondente esteve sempre ligada à história política e militar dos povos; dêstes, os primeiros de que se tem notícia documentada de terem feito uso de uma linguagem secreta foram os gregos e romanos.

Julio César, por exemplo, empregava um sistema em que as letras do texto claro eram substituídas por outras distantes quatro letras das primeiras. No século VX, entretanto, apareceu o pri-

meiro manual conhecido sôbre a arte de cifrar, de autoria de um secretário da cúria romana, assim como o primeiro tratado de decriptação (arte de decifrar a correspondência secreta sem o conhecimento das convenções respectivas), trabalho de um funcionário da chancelaria de Milão. Na época da Renascença, a criptografia teve um notável desenvolvimento com os italianos Cardano e Porta e o francês Vigenère. Foi no século XVII, porém, que esta arte atingiu o seu apogeu; diversas côrtes instalaram seus serviços de cifra, e os trabalhos de Bacon, Chanceler inglês, e do francês Rossignol, sob Luiz XIII, dão uma idéia da atividade que nesse sentido se desenvolvera na época. A celebridade de Rossignol foi tal como criptólogo e tão popular a sua fama que o seu nome veio a ser usado humorìsticamente como sinônimo de "gazua", passando mesmo para os dicionários franceses onde hoje é encontrado com essa significação.

Nos séculos XVIII e XIX assinalou-se certa decadência na arte dos cifrados. Nos exércitos de Napoleão, dizem que o emprêgo da criptografia era feito com certo descuido e a isso, em grande parte, se atribuem os revezes sofridos na Rússia pelo grande general, cuja correspondência cifrada era constantemente descoberta pelos russos, os maiores peritos na arte até nossos dias.

A mesma opinião existe em relação aos desastres franceses de 1870-71, quando eram deficientes as precauções adotadas no uso da criptografia. Em 1880, porém, há um verdadeiro despertar da arte, iniciando-se um movimento em que suas aplicações se multiplicaram e se aperfeiçoaram, surgindo publicações de caráter verdadeiramente científico, aparecendo o ensino oficial da criptografia não só em muitas escolas militares como em diversas chancelarias. Na grande guerra de 1914-18 novo impulso se deu à arte que evoluiu bruscamente talhada à feição das qualidades e defeitos da radiotelegrafia, exigindo um ambiente de cultura e trabalho para uma extraordinária tarefa que culminava na descoberta dos segredos do adversário lançados no espaço, sob a proteção dos mais hábeis e caprichosos artifícios, em um contínuo desafio à argúcia e à sua capacidade de trabalho. Para citar apenas um grande exemplo conhecido do papel da criptografia, temos o caso da batalha de Tannenberg, em agôsto de 1914, na qual os alemães obtiveram esmagadora vitória sôbre os russos. Ludendorff, com seu eficaz serviço criptográfico, ao qual comparecia pessoalmente, acabou por descobrir o segrêdo do serviço correspondente do inimigo e, assim, as comunicações expedidas pelo general em chefe russo eram conhecidas pelo general alemão. No atual conflito a criptografia tem tido um papel preponderante para ambos os contendores, facilitando à Alemanha seus golpes de surpresa sôbre a Polônia, Bélgica, Holanda e França, transmitindo ordens cifradas aos seus agentes diplomáticos nos citados países, instruindo-os quanto à ação dos "quinta-colunistas".

TIPOS DE CÓDIGOS

Denominam-se códigos, dicionários convencionalmente modificados, por meio dos quais unidades do texto, de comprimento variável, geralmente palavras, frases ou orações inteiras, podem ser substituídas por sinais arbitràriamente escolhidos, chamados *cifras, grupos* ou *palavras convencionais*. Seu emprêgo verificou-se no período de 1867 a 1870. Naquela época apenas eram conhecidas as mensagens em linguagem comum, inteligível, para a correspondência comum, e a em cifra (por métodos criptográficos diversos, que não o de códigos), tanto para os serviços diplomáticos como para os militares. Subseqüentemente apareceu o método de empregar na correspondência palavras que não correspondiam ao assunto tratado e cujo sentido só era conhecido pelos correspondentes que o empregavam. Êsse sistema foi aprovado, pela primeira vez, na Conferência Telegráfica Internacional de Roma, em 1871-1872. O primeiro código que se tornou largamente usado, em pouco tempo, foi o Código ABC, publicado em 1872, por W. Clauson-Thue. Embora defeituoso, logo se tornou universalmente conhecido devido à necessidade urgente de um código. Passou após por diversas melhorias, sendo ainda empregado até hoje.

Os códigos podem ser divididos em duas categorias, conforme sua elaboração: os *códigos em um volume*, que servem tanto para cifrar como para decifrar, e os *códigos em dois volumes*, que os franceses chamavam "à batons rompus", servindo um para cifrar e o outro para decifrar. O primeiro tipo geralmente é mais usado para códigos comerciais, sendo o segundo, devido a seu grau

de sigilo, preferido para os de tipo secreto. Dá isto, pois, lugar a uma outra classificação dos códigos, isto é: códigos comerciais e códigos secretos.

Códigos comerciais — Desde 1904 os tipos mais antigos de códigos foram quase completamente suplantados por códigos constituídos por grupos de cinco letras, formados por meio de *tábuas de arranjos* cuidadosamente elaboradas. Estas tábuas fecilitam a elaboração de séries de 100.000 ou mais "palavras convencionais" de cinco letras, tôdas diferindo uma da outra em pelo menos duas letras. São dêsse tipo o célebre código inglês "Bentley", "Código Mascote" e os nossos códigos "Borges" e "Código Telecriptográfico Brasil".

Códigos secretos — Os códigos secretos seguem, em grande parte, os modelos sugeridos pelos códigos comerciais, mas nêles há preponderância do tipo de "batons rompus", com cifrador e decifrador, sendo também usado o código com grupos de algarismos. Na estrutura de um código, após o prefácio, introdução, e em certos casos a descrição da estrutura e instruções para o seu uso, vem também o texto, pròpriamente dito, na primeira coluna do qual, geralmente, são colocados números ordinários, vindo depois, na segunda coluna, as palavras convencionais de cinco letras em ordem alfabética e, finalmente, numa terceira coluna, as palavras, expressões ou orações. Pràticamente, em tôdas as expressões ou orações há uma palavra principal. São estas palavras que, na terceira coluna, são colocadas em rigorosa ordem alfabética, juntamente com as palavras desacompanhadas de frases. Estas últimas são colocadas em seguida à palavra principal correspondente, obedecendo a colocação de umas em relação às outras à ordem alfabética. Além do vocabulário, contém um código as denominadas tabelas. Estas se referem a números, preços, nomes de companhias, personalidades e tabelas gramaticais. Fogem elas, em geral, à ordem alfabética e sua colocação nos códigos dá-se tanto no início como no fim, como também é indicado no índice. Nos atuais códigos as palavras convencionais, ou sejam as cifras, são compostas de cinco letras apenas, pela resolução da Conferência de Madrid de 1932, que veio abolir o sistema de dez letras permitido pela Convenção de Bruxelas de 1928.

COMPLICADORES — VARIEDADES

Dadas as palavras convencionais de um código, pode-se aplicar-lhes um processo criptográfico qualquer de modo a transformar essas palavras e torná-las irreconhecíveis, exceto para os operadores que estejam no conhecimento do processo empregado. A operação chama-se *complicar* e o processo requer, às vêzes, o emprêgo de tabelas especiais chamadas *complicadores*. O seu fim é dificultar o trabalho dos analistas de códigos e a aumentar o seu sigilo, sendo empregados na correspondência confidencial ou secreta. Os complicadores pertencem ao sistema criptográfico chamado de substituição e consistem geralmente em tabelas tendo por fim: 1.º) transformar elementos das "palavras convencionais", compostas de letras, em outras "palavras convencionais", também de letras; 2.º) transformar as palavras convencionais de algarismos em outras palavras convencionais de algarismos; 3.º) transformar algarismos em letras; e, finalmente, 4.º) transformar letras em algarismos. As duas últimas variedades constituem o que se chama *transformadores* pròpriamente ditos. Os complicadores nos quais o número de elementos de correspondência é de dois (algarismos ou letras) apresentam-se geralmente sob a forma de quadros, contendo todos os arranjos das 26 letras, duas a duas, ou dos 10 algarismos, dois a dois. Êste sistema é conhecido em criptografia pelo nome de substituição por poligramas, no caso presente *bigramas*, isto é, duas letras. O complicador assume então o aspecto de um quadro no qual as primeiras letras dos bigramas figuram sôbre uma linha horizontal, as segundas letras sôbre uma coluna vertical, ou vice-versa, e no qual cada quadrado contém um grupo de duas letras ou três algarismos representando o bigrama definido pela coluna e pela linha.

Exemplo:

	A	B	C	D	E
A	001	002	003	004	005
B	027	028	029	030	031
C	053	054	055	056	057
D	079	080	081	082	083
E	109	106	107	108	109

O bigrama CA é substituído por 003; DE por 108, etc., etc..

Finalmente, pode-se dizer que o princípio geral a que obedecem os complicadores é a representação dos grupos de letras ou algarismos por suas coordenadas que determinam a sua posição nos quadros em que estão escritos. Êsses grupos de letras ou algarismos podem ser as próprias palavras convencionais do código que se escreverão seguidamente da primeira à última, em quadros diversos numerados ou designados por letras. Observe-se, no entanto, que se pode complicar um texto cifrado sem o uso pròpriamente dito de complicadores, adotando-se qualquer dos inúmeros processos usados em criptografia, como por exemplo o sistema de transposição pela adição de um mesmo número às palavras convencionais em algarismos, etc..

PASSAGEM DO TEXTO EM CLARO PARA LINGUAGEM TELEGRÁFICA — CIFRAÇÃO — DECIFRAÇÃO — COMPLEMENTO DO TEXTO TELEGRÁFICO

(PARÁFRASE)

Transormar um texto escrito na linguagem ordinária ou comum em outro texto redigido em linguagem convencional e sem um significado aparente à primeira vista, é o que se chama cifrar o texto. A operação contrária, ou seja transformar um criptograma em texto claro que lhe deu origem, chama-se decifrar o criptograma. Poucas são as regras fundamentais que devem ser observadas, em todo trabalho criptográfico; qualquer omissão, porém, na observância de tais regras, conduzirá, inevitàvelmente, à descoberta do código, ou cifra, por terceiros. Grande êxito dos cripto-analistas (peritos em decifrar criptogramas de terceiros) deve-se à ignorância e descuido dos funcionários encarregados de transformar os telegramas de linguagem clara em código ou cifra. Ao cifrar um texto deve o criptógrafo fazer sempre a máxima economia de palavras, sem alterar, evidentemente, o sentido do mesmo, procurando, outrossim, empregar as frases feitas que se encontrem porventura nos códigos. Para segurança dêstes, o telegrama cifrado nunca deve ser repetido em qualquer outra forma ou cifra e muito menos em linguagem clara, assim como não poderá ser repetido, retransmitido ou respondido em código o telegrama que já tenha sido transmitido em claro. Num criptograma, nunca se deverá inserir palavras em linguagem clara, pois muito facilitará a tarefa dos cripto-analistas, assim como o fornecimento de cópia textual de um telegrama em código implicará na quebra de sigilo do mesmo, como também qualquer informação, mesmo cifrada, relativa ao processo criptográfico adotado. Se for necessário retransmitir um mesmo telegrama em outro código, para reexpedí-lo será preciso parafrasear o seu texto antes de cifrá-lo novamente, ou melhor, reescrevê-lo mudando as palavras originais, tanto quanto possível, sem alterar-lhe o sentido. Isso é feito invertendo-se a posição das frases, do sujeito, do predicado e modificando as frases ou orações do período; alterando-se a linguagem, sem perda do sentido; suprimindo-se ou adicionando-se palavras, de preferência a ampliar o telegrama. Depois de parafraseado, poderá o telegrama ser expedido em outra chave ou código. Ao decifrar um criptograma deverá, também, ficar ao critério do criptógrafo parafraseá-lo, procurando ampliá-lo de maneira que seu texto se torne claro e o sentido perfeito. Quanto maiores forem o número e a extensão dos telegramas, mais depressa poderão ser descobertas as cifras; portanto, a formação e adoção de formas fixas, ou melhor, a repetição constante de uma mesma cifra no mesmo criptograma deve ser evitada. Finalmente, a prática na elaboração dos telegramas em código é especialmente recomendada, desenvolvendo-se assim, ràpidamente, a desejável familiaridade com as palavras próprias e frases contidas no código. Êsse fator conduz à maior rapidez na operação, tanto de cifração como decifração, permitindo reduzir consideràvelmente a extensão dos telegramas, bem como o tempo necessário à sua preparação.

O CRIPTÓGRAFO — CONDIÇÕES DE PREFERÊNCIA QUANTO AO SEXO, IDADE E TEMPERAMENTO (PRECISÃO, ATENÇÃO E DISCREÇÃO)

Compete aos criptógrafos a cifração e a decifração dos criptogramas, parafraseá-los e após submetê-los à apreciação dos chefes.

É portanto de grande importância para as chancelarias possuírem um quadro de técnicos especializados nessa função, pois sòmente depois de alguns anos de prática poderá um criptógrafo demonstrar tôda sua eficiência. Cabe a êstes, também, rever e atualizar, periòdicamente, os códigos

em vigor, alterando ou substituindo por outras as expressões fora de uso, enriquecendo seu texto com nomes de personalidades do momento, etc., assim como apresentar sugestões quanto à transmissão e sigilo dos criptogramas.

Tratando-se, pois, de um cargo no qual estará a par, constantemente, de comunicações de caráter político, confidencial e secreto, o ingresso ao cargo exigirá notòriamente requisitos morais, como discreção, noção de responsabilidade, seriedade, precisão, atenção e paciência. No entretanto, o "test" mais eficiente para esclarecer se o criptógrafo possui tais qualidades é realmente o estágio probatório. É mediante êste que o criptógrafo poderá demonstrar se, além das qualidades intelectuais, possui, igualmente, as de ordem moral, tão importantes quanto aquelas.

Quanto ao sexo, várias chancelarias têm utilizado criptógrafos do sexo feminino a pleno contento de seus dirigentes, inclusive o Itamaratí, tendo-se revelado, inúmeras vezes, superior ao masculino, não só quanto à capacidade de trabalho, tirocínio, noção de responsabilidade, critério e mesmo discreção. Portanto, o cargo poderá ser exercido quer por um quer por outro, contando que preencha as qualidades acima referidas.

Quanto ao estado civil, podem ser os criptógrafos, quer masculinos, quer femininos, casados, mas sempre com nacional do país. No entretanto, os solteiros já exercendo o cargo, quando pretenderem contrair núpcias, deverão, a exemplo da carreira de "Diplomata", pedir autorização, pois, como é sabido, o casamento altera substancialmente as condições de vida das pessoas, estabelecendo, por meio dêle, uma íntima união de interêsses entre os cônjuges, não só de ordem econômica, como social e moral.

Quanto à idade, tratando-se de cargo de grande responsabilidade, não deverá ser inferior a 21 e superior a 35 anos para os candidatos desempenharem tal função.

A VIOLAÇÃO DOS CÓDIGOS E AS CÂMARAS NEGRAS

A violação dos códigos por processos sistemáticos é levada a cabo por meio da *análise criptográfica*. Dadas as características conhecidas de certos códigos comerciais, é possível reconhecer-se se o texto foi cifrado por alguns dêles. Mas quando se ignora, não sòmente o código, seu tipo, como também a língua usada pelos correspondentes, o problema torna-se extremamente complicado. Para solver o problema da violação dos códigos cuja solução se torna de primeira necessidade, não só na guerra como na paz, têm sido criados "escritórios de análise criptográfica". Assim, nos Estados Unidos da América, durante e mesmo após a guerra de 1914-18, foi criado um escritório dêste gênero que se ocultava sob o nome de "Black Chamber" e que, segundo a exposição publicada pelo seu diretor sob o título "The American Black Chamber", alcançou os mais surpreendentes resultados.

O primeiro exame que se deve fazer num criptograma tem por fim descobrir se não terá sido empregado um complicador e se se conhece o código empregado. Procurar-se-ão, para isso, as repetições de grupos ou de fragmentos de grupos, fazendo, se necessário, uma estatística sumária por colunas, de acôrdo com o primeiro algarismo (ou letra) de cada grupo (todos os grupos que comecem por O, todos que comecem por 1, etc.) ou então, se se supõe, depois de algumas repetições, a existência de grupos de 4 ou 3 caracteres colocados em seguida uns aos outros, faz-se a estatística segundo o primeiro algarismo (ou letra) dêsses grupos. Se não se encontram repetições, deve-se temer o emprêgo do complicador. No caso de haver repetições e de não se saber se o código empregado é ou não secreto, procura-se o repertório dos grupos freqüentes nos códigos conhecidos. Se nestes não se encontrarem essas palavras muito freqüentes, pode-se formar hipóteses para serem verificadas posteriormente. É razoável, por exemplo, que a cifra repetida se refira ao ponto final ou a conjunção e. A pesquisa, no entanto, é grandemente facilitada quando se tem hipóteses sôbre o sentido da palavra representada pelo grupo. Ora, a presença de *palavras em claro* facilita muito essas hipóteses e sua presença garante ao criptoanalista que não foi empregado um método de complicar o texto da espécie dos que alteram a totalidade do criptograma. Também dá a conhecer a língua empregada nas partes cifradas, facilitando, também, hipóteses quanto ao assunto tratado. Outras bases que favorecem ainda a formação de hipóteses são os *telegramas nos mesmos têrmos, grupos iniciais repetidos* em diversos telegramas, os descuidos e as indiscreções dos criptógrafos, como também, os *assuntos do dia*. Nesta última hipótese, por exemplo, na correspondência

diplomática, os acontecimentos mundiais fazem com que, nos telegramas das chancelarias aos representantes diplomáticos, ou dêstes para aquelas, apareçam constantemente nomes em evidência. Na correspondência entre a Embaixada dos Estados Unidos da América em Londres e o Departamento de Estado deve-se supor que as palavras muito repetidas devam referir-se aos nomes de Roosevelt, Churchill, Stalin, Hitler, Eisenhower, etc., no atual momento.

É preciso observar, no entanto, que antes de se aventurar hipóteses sôbre o significado dos grupos repetidos num criptograma é preciso decidir-se a preliminar de se o texto foi cifrado por um sistema criptográfico ou por meio de um código, distinção esta que só pode ser feita por peritos. Edgard Allan Poe asseverou que "pode ser assegurado, de um modo geral, que o engenho humano não pode inventar um sistema de cifras que o engenho humano não possa desvendar". William F. Friedman, Chefe da Secção de Cifras e Códigos do Departamento de Guerra dos Estados Unidos da América, acha que essa afirmação só é verdadeira se se aplicar a sistemas empregados repetidamente em uma correspondência muito volumosa, pois que, *"criptogramas curtos, preparados por certos métodos, podem resistir indefinidamente à cripto-análise"*.

OS PROCESSOS MECÂNICOS — RESTRIÇÕES À SUA APLICAÇÃO

Máquinas para facilitar operações sôbre cifras são conhecidas há muitos anos; variam em complexidade desde simples discos, superpostos e concêntricamente ou excêntricamente rotarórios, até aparelhos de máquinas de escrever, que funcionam elètricamente, modificados apropriadamente para fins criptográficos. Entre os melhores e mais conhecidos aparelhos criptográficos do tipo mais simples e mecânico, além do "Aparelho Wheatstone", conta-se o do francês Bazeries, cuja invenção data do ano de 1891. O cilindro Bazeries consiste numa série de vinte discos, trazendo cada um na sua periferia um alfabeto desordenado diferente. Os discos, que trazem números identificadores, de 1 a 20, são reunidos num eixo comum da esquerda para a direita, segundo uma chave numérica. Na cifração os discos são rodados, ou melhor, girados de modo a levar as letras do texto em claro a formar uma única linha horizontal e então as letras de qualquer outra linha horizontal são tomadas como cifras equivalentes. O texto é assim cifrado em 20 letras de cada vez. Para decifrar, as letras-cifras são colocadas numa linha horizontal, girando os discos e fixando-os na posição necessária. Girando o cilindro lentamente e examinando todas as linhas horizontais, poder-se-á ver que só uma destas dá um texto inteligível. No entretanto, o princípio no qual foi baseado foi concebido muitos anos antes por Thomas Jefferson. Um dos mais engenhosos e complicados tipos de máquinas cifradoras é o constituído por certo aparelho telegráfico de feitio moderno. Neste sistema a cifração elétrica, a transmissão, a recepção e a decifração, controladas por fitas perfuradas, podem ser efetuadas simultâneamente com um grau elevado de presteza. Dos muitos dispositivos e máquinas que têm sido inventados, construídos e postos no mercado, sòmente um número diminuto está atualmente em uso, dentre êles o aparelho brevetado por "Aktrebolaget-Cryptograph", de Estocolmo, e várias máquinas da "Patent DeveloPping Company". No entretanto, apesar do grande número de combinações que poderá oferecer qualquer destas máquinas, além do seu mecanismo delicado e complicado, de fácil desarranjo, o grau de sigilo não é suficientemente alto para permitir a sua adoção na correspondência diplomática, militar ou naval.