Criptografia: Origens

SEGA4 – Segurança da informação

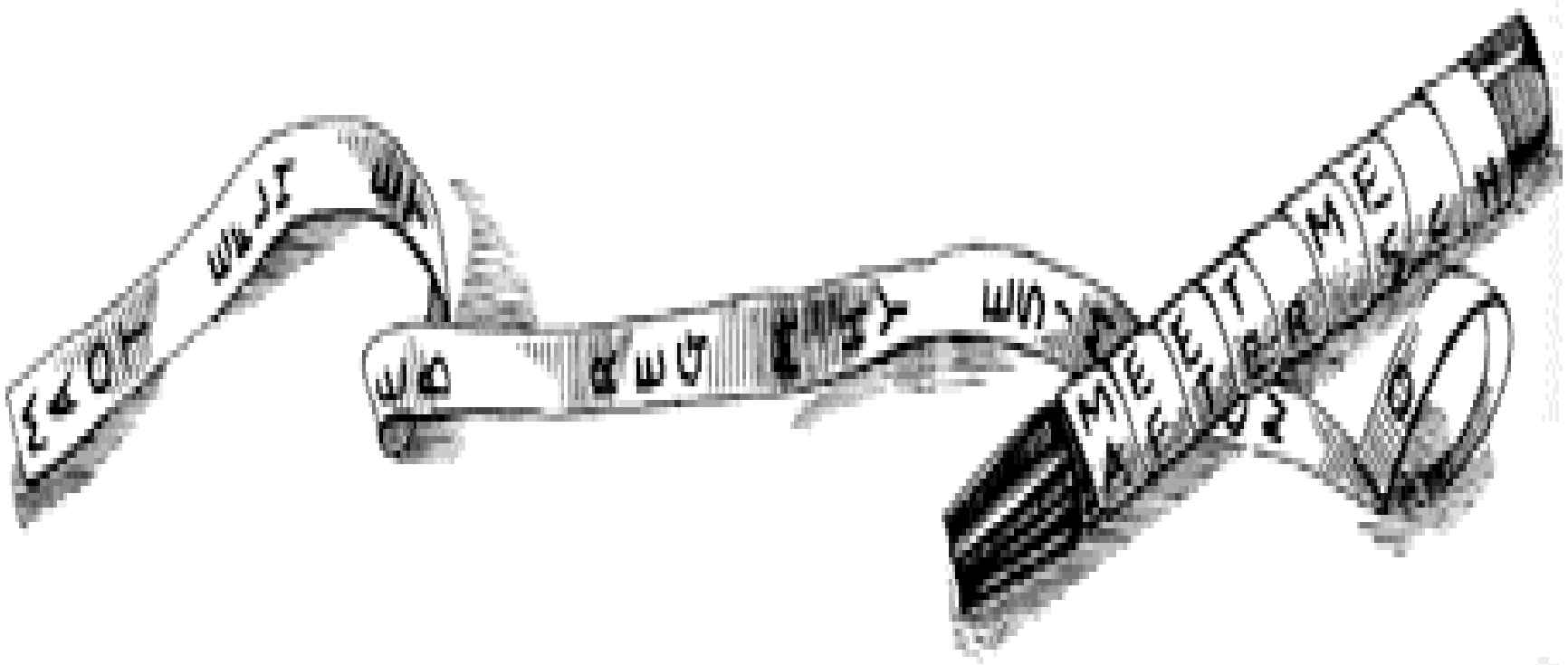
Objetivos da aula

- Conhecer aspectos históricos da criptografia.
- Conhecer a importância da criptografia na história da civilização.
- Conhecer alguns dos principais dispositivos criptográficos até o nascimento dos computadores digitais.
- Conhecer a máquina Enigma.

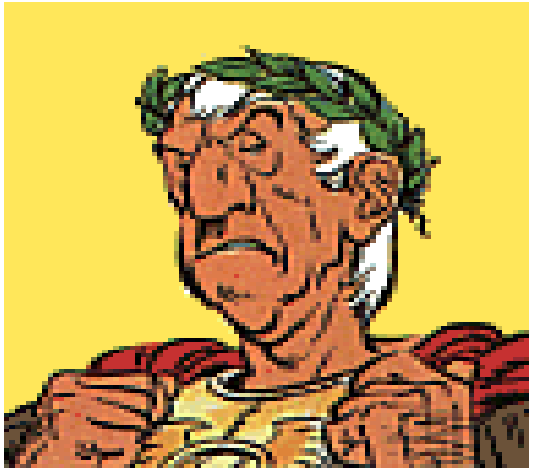
Origens

- Antiguidade
  - Egípcios substituiam palavras em documentos para evitar identificação de tumbas.
  - Mesopotâmios codificavam fórmulas de produtos.
  - Livro de Jeremias documenta utilização de codificação com substituição simples.
  - Relógio de água grego para transmitir mensagens para longas distâncias.

Bastão de Licurgo



Código de César



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

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

Cifragem por deslocamento

- O número de chaves possível é 26.
- É facil decifrar uma mensagem através análise de frequências.

Exemplo

BPMZM WVKM EIA IV COTG LCKSTQVO

EQBP NMIBPMZA ITT ABCJJG IVL JZWEV

IVL BPM WBPMZ JQZLA AIQL QV AW UIVG EWZLA

OMB WCB WN BWEV

OMB WCB, OMB WCB, OMB WCB WN BWEV

IVL PM EMVB EQBP I YCIKS IVL I EILLTM IVL I YCIKS

QV I NTCZZG WN MQLMZLWEV

BPIB XWWZ TQBBTM COTG LCKSTQVO

EMVB EIVLMZQVO NIZ IVL VMIZ

JCB IB MDMZG XTIKM BPMG AIQL BW PQA NIKM

VWE OMB WCB, OMB WCB, OMB WCB WN PMZM

IVL PM EMVB EQBP I YCIKS IVL I EILLTM IVL I YCIKS

IVL I DMZG CVPIXXG BMIZ

Underlying Plain Text

Cipher Text

The shift of E seems to be either 4, 8, 17, 18 or 23

The shift of A seems to be either 1, 8, 12, 21 or 22

There once was an ugly duckling
With feathers all stubby and brown
And the other birds said in so many words
Get out of town
Get out, get out, get out of town
And he went with a quack and a waddle and a quack
In a flurry of eiderdown
That poor little ugly duckling
Went wandering far and near
But at every place they said to his face
Now get out, get out, get out of here
And he went with a quack and a waddle and a quack
And a very unhappy tear

Idade média

- Árabes inventam a criptoanálise
  - Al-Kindi: escreveu livro sobre decifração de mensagens criptográficas.
  - Ibrahim Dunainir descreve a transmissão de mensagens utilizando cifras algébricas.

Cifragem por substituição

ABCDEFGHIJKLMNOPQRSTUVWXYZ
TMKGOYDSIPELUAVCRJWXZNHBQF

Hence HELLO encrypts to SOLLV

O número de chaves é 26! ~2^{88}

Frequências da língua inglesa

The most common bigrams are, in decreasing order,

- TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA

The most common trigrams are, in decreasing order,

- THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR

XSO MJIWXVL JODIVA STW VAO VY OZJVCO'W LTJDOWX KVAKOAXJTXIVAW VY SIDS XOKSAVLVDQ IAGZWXJQ.KVUCZXOJW, KVUUZAIKTXIVAW TAG UIKJVOLOKXJVAIKW TJO HOLL JOCJOWOAXOG, TLVADWIGO GIDIXTL UOGIT, KVUCZXOJ DTUOW TAG OLOKXJVAIK KVUUOJKO. TW HOLL TW SVWXIAD UTAQ JOWOTJKS TAG CJVGZKX GONOLVCUOAX KOAXJOW VY UTPVJ DLVMTL KVUCTAIOW, XSO JODIVA STW T JTCIGLQ DJVHIAD AZUMOJ VY IAAVNTXINO AOH KVUCTAIOW. XSO KVUCZXOJ WKIOAKO GOCTJXUOAX STW KLVWO JOLTXIVAWSICW HIXS UTAQ VY XSOWO VJDTAIWTXIVAW NIT KVLLTMVJTXINO CJVPOKXW, WXTYY WOKVAGUOAXW TAG NIWIXIAD IAGZWXJITL WXTYY. IX STW JOKOAXLQ IAXJVGZKOG WONOJTL UOKSTAIWUW YVJ GONOLVCIAD TAG WZCCVJXIAD OAXJOCJOAOZJITL WXZGOAXW TAG WXTYY, TAG TIUW XV CLTQ T WIDAIYIKTAX JVLO IA XSO GONOLVCUOAX VY SIDS-XOKSAVLVDQ IAGZWXJQ IA XSO JODIVA.

XSO GOCTJXUOAX STW T LTJDO CJVDJTUUO VY JOWOTJKS WZCCVJXOG MQ IAGZWXJQ, XSO OZJVCOTA ZAIVA, TAG ZE DVNOJAUOAX JOWOTJKS OWXTMLIWSUOAXW TAG CZMLIK KVJCVJTXIVAW. T EOQ OLOUOAX VY XSIW IW XSO WXJVAD LIAEW XSTX XSO GOCTJXUOAX STW HIXS XSO KVUCZXOJ, KVUUZAIKTXIVAW, UIKJVOLOKXJVAIKW TAG UOGIT IAGZWXJIOW IA XSO MJIWXVL JODIVA . XSO TKTGOUIK JOWOTJKS CJVDJTUUO IW VJDTAIWOG IAXV WONOA DJVZCW, LTADZTDOW TAG TJKSIXOKXZJO, GIDIXTL UOGIT, UVMILO TAG HOTJTMLO KVUCZXIAD, UTKSIAO LOTJAIAD, RZTAXZU KVUCZXIAD, WQWXOU NOJIYIKTXIVA, TAG KJQCXVDJTCSQ TAG IAYVJUTXIVA WOKZJIXQ.

We have the following statistics for single letters

Letter	Freq	Letter	Freq	Letter	Freq
A	8.6995	B	0.0000	C	3.0493
D	3.1390	E	0.2690	F	0.0000
G	3.6771	H	0.6278	I	7.8923
J	7.0852	K	4.6636	L	3.5874
M	0.8968	N	1.0762	O	11.479
P	0.1793	Q	1.3452	R	0.0896
S	3.5874	T	8.0717	U	4.1255
V	7.2645	W	6.6367	X	8.0717
Y	1.6143	Z	2.7802		

Most common bigrams : TA, AX, IA, VA, WX, XS, AG, OA, JO, JV

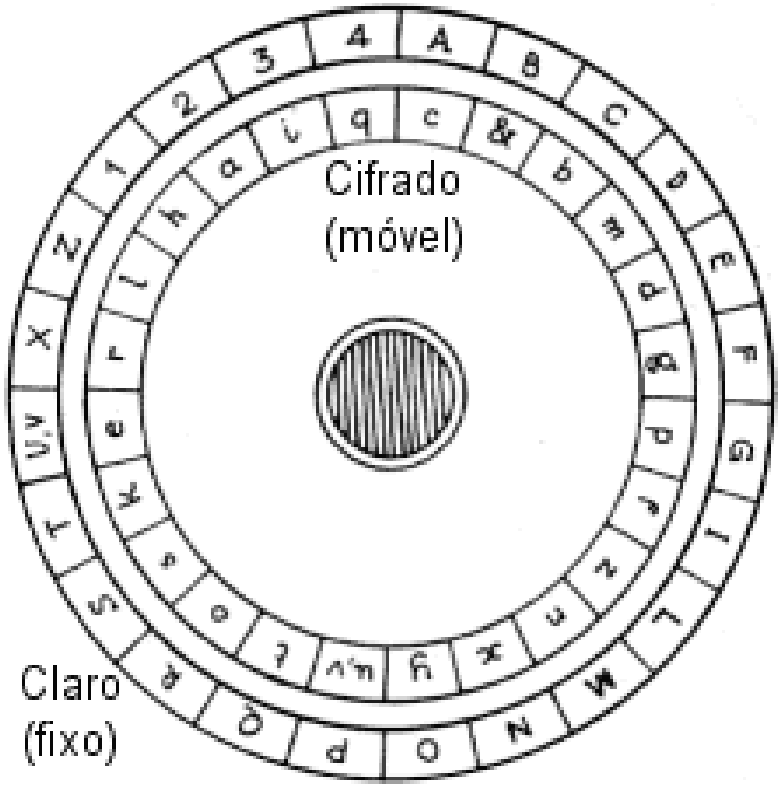
Most common trigrams : OAX, TAG, IVA, XSO, KVU, TXI, UOA, AXS

Exemplo de análise

- Uma boa hipótese é O = E
- Os trigramas mais comuns são
  - OAX = E * *
  - XSO = * * E
- Os trigramas mais comuns são: ENT, ETH e THE
- Assim existe uma grande possibilidade que:
  - X=T
  - S=H
  - A=N

Idade Moderna

- Leon Alberti – (1404-1472)
- Disco de cifragem (Substituição polialfabética)



Código de Vigenére

- Blaise Vigenére (1523-1596)
- Vigenére cria um sistema de cifragem polialfabético considerado inquebrável.
- Entretanto, por vários séculos não foi utilizado por ter sido considerado muito complexo para ser utilizado.

Tabela de Vigenére

ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCDEFG
IJKLMNOPQRSTUVWXYZABCDEFGH
JKLMNOPQRSTUVWXYZABCDEFGHI
KLMNOPQRSTUVWXYZABCDEFGHIJ
LMNOPQRSTUVWXYZABCDEFGHIJK
MNOPQRSTUVWXYZABCDEFGHIJKL
NOPQRSTUVWXYZABCDEFGHIJKLM
OPQRSTUVWXYZABCDEFGHIJKLMN
PQRSTUVWXYZABCDEFGHIJKLMNO
QRSTUVWXYZABCDEFGHIJKLMNOP
RSTUVWXYZABCDEFGHIJKLMNOPQ
STUVWXYZABCDEFGHIJKLMNOPQR
TUVWXYZABCDEFGHIJKLMNOPQRS
UVWXYZABCDEFGHIJKLMNOPQRST
VWXYZABCDEFGHIJKLMNOPQRSTU
WXYZABCDEFGHIJKLMNOPQRSTUV
XYZABCDEFGHIJKLMNOPQRSTUVW
YZABCDEFGHIJKLMNOPQRSTUVWX
ZABCDEFGHIJKLMNOPQRSTUVWXY

Exemplo

Key letters:	P	Y	R	A	M	I		D	P		Y	R	A	M	I		D	P
plaintext:	A	T	T	A	C	K		A	T		S	U	N	D	O		W	N
Crypto:	P	R	K	A	O	S		D	I		Q	L	N	P	W		Z	C

Babbage

- Babbage quebra o código de Vigenére em 1854.
- Oficialmente o código de Vigenére foi quebrado por Kasiski em 1863.
- Babbage possivelmente manteve o segredo de sua descoberta por pressões do governo britânico.

Processo para quebrar o código de Vigenére

1. Descobrir o tamanho da chave
    1. Identificar sequências repetitivas.
    2. A partir das distâncias deduzir o tamanho da chave utilizada.
2. A partir do tamanho da chave aplicar a análise de frequência nas sequências de letras criadas de acordo com a distância das letras.

Idéia

K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G	K	I	N	G
T	H	E	S	U	N	A	N	D	T	H	E	M	A	N	I	N	T	H	E	M	O	O	N
D	P	R	Y	E	V	N	T	N	B	U	K	W	I	A	O	X	B	U	K	W	W	B	T

One-time-pad (ou código de Vernam)

- Um código difícil de ser quebrado (mesmo com a tecnologia atual) é o código de Vernam.
- Nesse código o tamanho da chave é o mesmo da mensagem.
- Se a chave for um texto aleatório, o texto cifrado também será um texto aleatório.
- O problema desta técnica é a dificuldade de uso.

Cont.

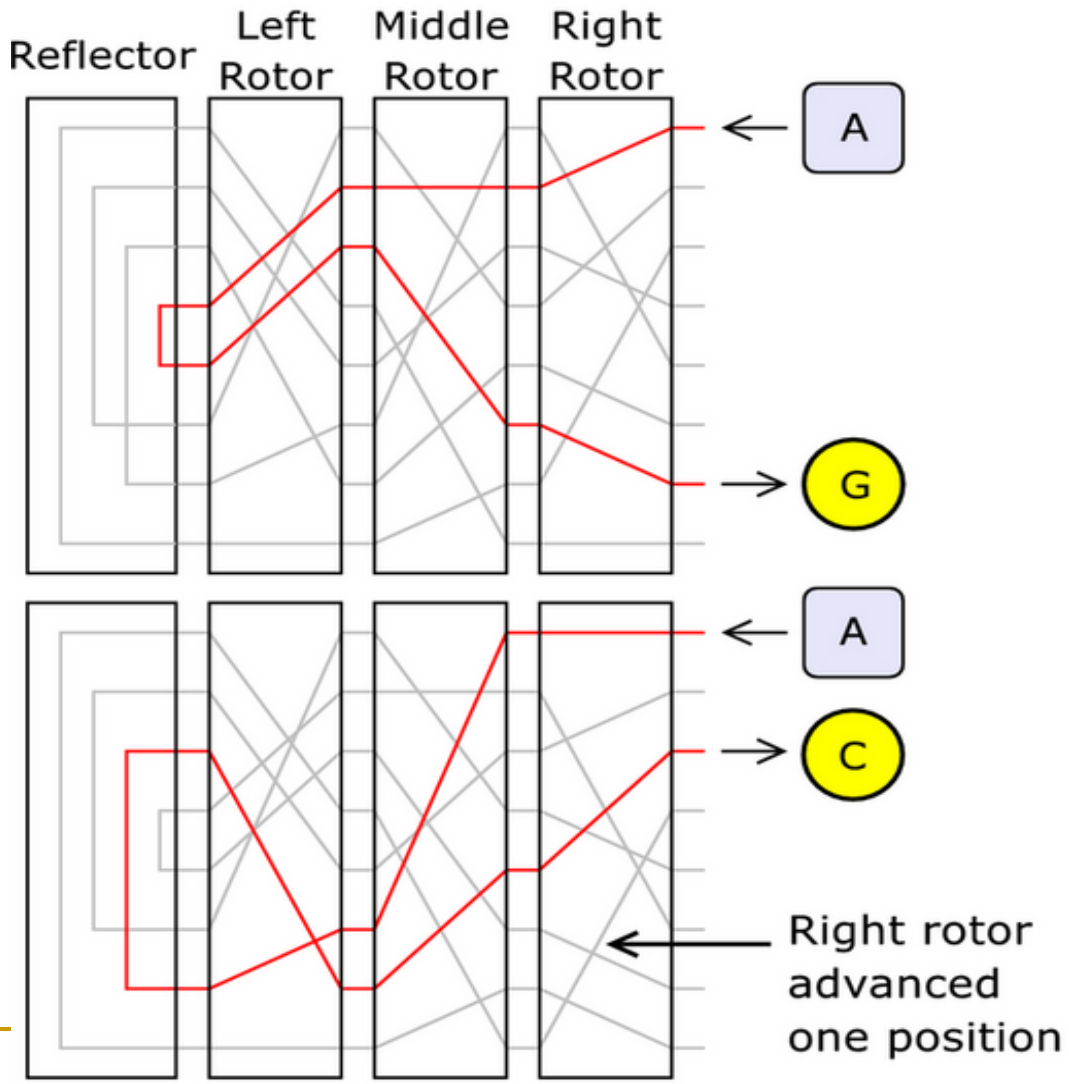
- O código de Vernam foi utilizado em conjunto com o código Morse.
- Para cada mensagem enviada existia uma chave do tamanho da mensagem. O processo era mecanizado através do uso de fitas perfuradas.

Enigma

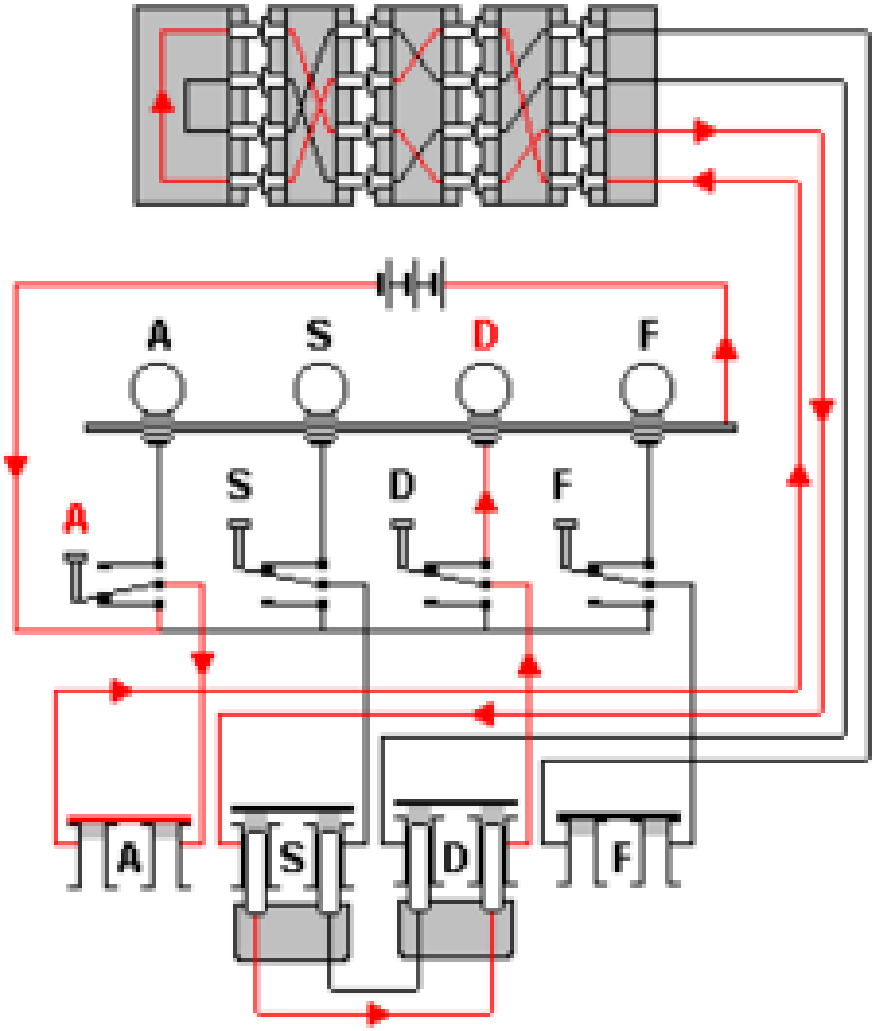
História

- Criado e patenteado por Arthur Scherbius em 1918.
- Inicialmente foi um fracasso comercial. As instituições financeiras não tiveram interesse em utilizar essa tecnologia.
- Nos anos 30 os militares alemães adotaram e aperfeiçoaram o modelo comercial.

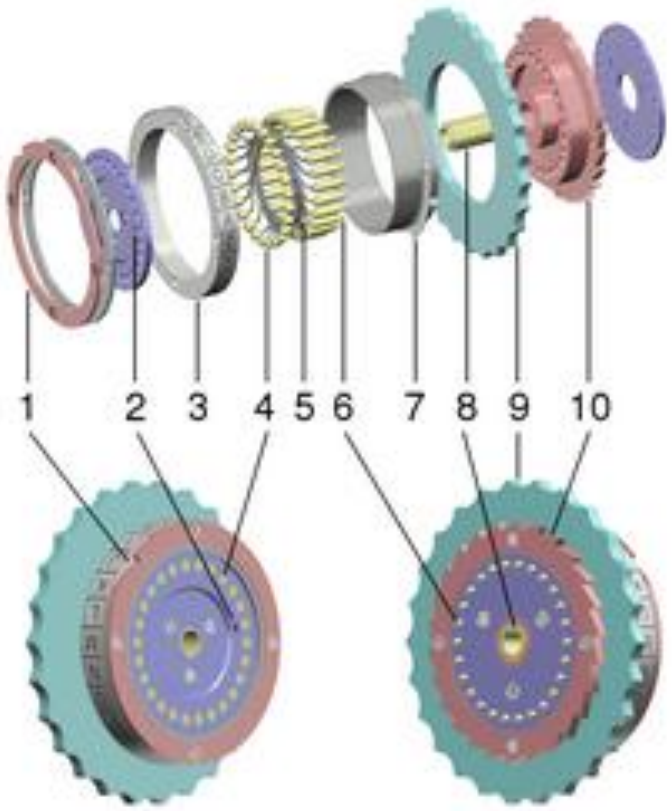
Descrição


Reflector
Left Rotor
Middle Rotor
Right Rotor
A
G
A
C
Right rotor advanced one position

Esquema elétrico



Rotores



Plugboard

Número de chaves possíveis

- Posição inicial dos rotores:
  - 17.576
- Arranjos dos rotores:
  - 6
- Plugboard:
  - 100.391.791.500
- Total
  - 17.576 * 6 * 100.391.791.500 ~= 10^{16}

Procedimento de uso

- Cada operador possuia um livro de chaves atualizado periodicamente.
- Todas as manhãs os operadores atualizavam os seus equipamentos conforme a chave do dia.
- Para cada mensagem era selecionada uma chave diferente.
- A chave da mensagem era enviada utilizando-se a chave do dia.

Quebra do Enigma

- A quebra do Enigma foi um fato significativo para a definição do resultado da 2.a Guerra Mundial.
  - Posições de submarinos alemães.
  - Destruição de suprimentos para a África do Norte.
  - Batalhas de Stalingrado e Kursk.

Abordagem matemática

- A Polônia desde a sua independência via a Alemanha como uma grande ameaça e necessitava acompanhar de perto o desenvolvimento militar alemão.
- O serviço secreto polônes estabelece um grupo de criptoanálise recrutando matemáticos poloneses com domínio da língua alemã.

Marian Rejewski

- Rejewski inicialmente quebra o código do Enigma explorando uma falha de procedimento de enviar de forma repetida a chave da mensagem no início de cada mensagem.
- Exemplo: QRSQRS seria criptografado como JXDRFT. De modo que (J,R), (X,F) e (D,T) estão relacionados.

Bletchley Park

- A Polônia passa o conhecimento adquirido sobre o Enigma para a Inglaterra e a França.
- Os ingleses concentram o esforço de quebra da máquina Enigma em um centro em Bletchley Park.

Falhas do enigma

- O Enigma tem uma falha fundamental: Uma letra nunca poderia ser codificada para ela mesma. Explorando esta falha seria possível identificar palavras candidatas para uma palavra suspeita. Por exemplo, todas as manhãs, as estações meteorológicas enviavam mensagens sobre o tempo. Sobre estas mensagens eram analisadas palavras relativas a tempo e posição.

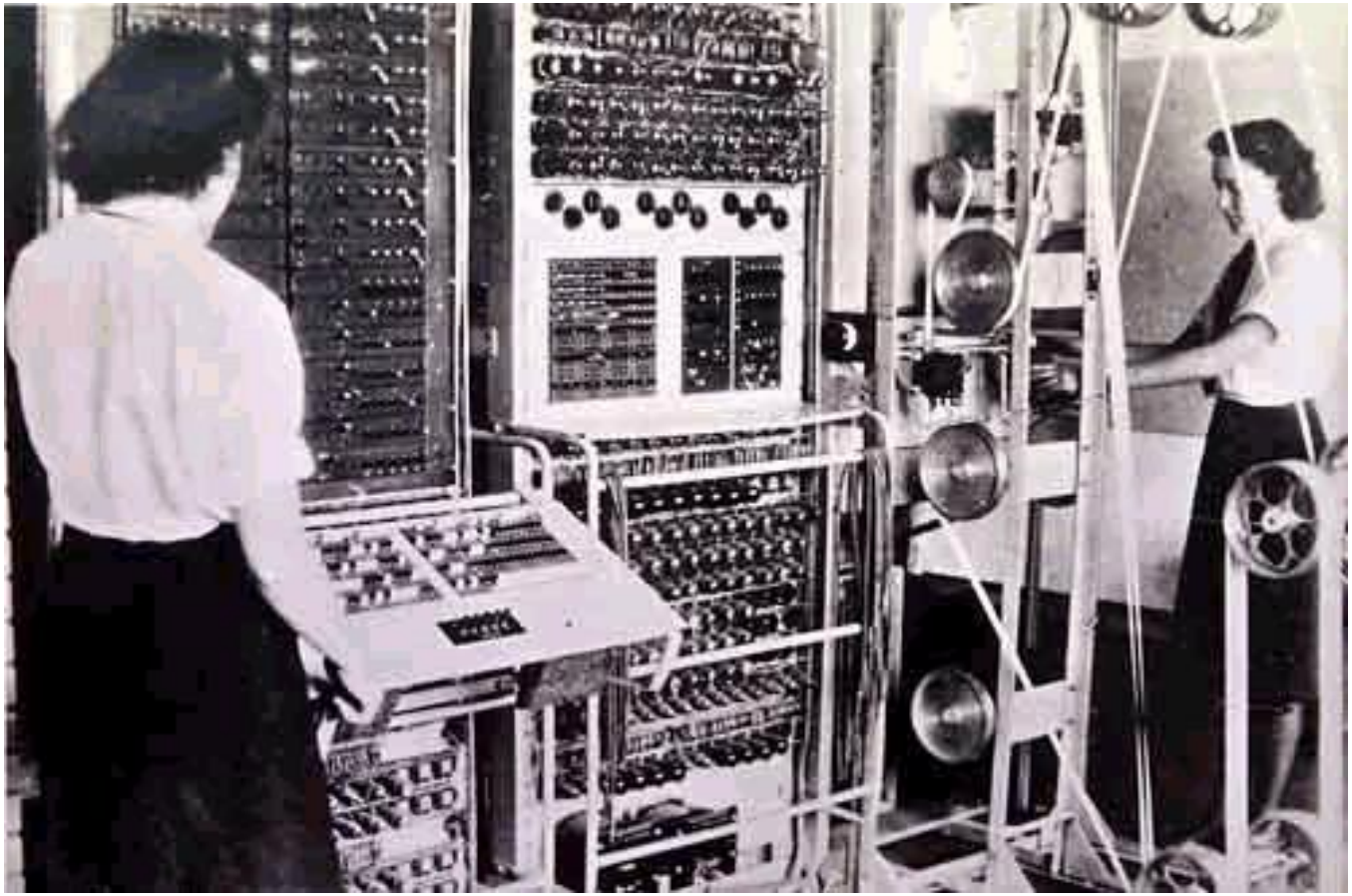
Cont.

- Deficiências operacionais:
  - Operadores frequentemente repetiam chaves de mensagens.
  - Regras sobre plugboards tais como não utilizar letras vizinhas.
  - Operadores nem sempre seguiam regras para destruição de livros e equipamento.
- Principal deficiência:
  - **Excesso de confiança!!!**

Método de quebra do Enigma

- Ver Codebook

Colossus (1.o computador ?)



Após a 2.a guerra

- O governo britânico mandou destruir todos os equipamentos referentes a quebra do Enigma. Medo que esse conhecimento chegasse aos soviéticos.
- Turing se suicida na prisão.

Aprendizado para a situação corrente

- Principais defeitos:
  - Known Plain text attack.
  - Gestão de chaves deficiente.
- Pessoal é o elo mais fraco do sistema
  - Corrupção.
  - Falta de treinamento adequado.
- Nunca subestimar a quantidade de recursos que o oponente está disposto a gastar.
  - O esforço de criptoanálise do Enigma envolveu milhares de pessoas, planejamento detalhado e uma grande visão estratégica.

Conclusões

- Segurança de informação é uma necessidade básica da civilização.
- Desenvolvimentos em criptografia são frutos diretos de esforços de confrontos militares.
- Excesso de confiança na tecnologia pode ser a maior vulnerabilidade de um sistema.
- O fator humano é geralmente o elo mais fraco do sistema.

Próxima aula

- Criptografia simétrica.