Apresentação

SEGURANÇA INFORMÁTICA

INVERNO 2023-2024

ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

Objectivos

Realizar uma introdução à teoria e prática da segurança informática

Teoria	Prática
• mecanismos criptográficos, modelos de controlo de acesso, …	• utilização de API criptográficas, configuração de sistemas, …

Fornecer a base conceptual e prática necessária ao estudo dos aspectos de segurança em contextos específicos

Sistemas distribuídos	Sistemas de informação	Redes de comunicação de dados

2

Programa

Parte I – Mecanismos e Protocolos Criptográficos

- Esquemas criptográficos
- Métodos para autenticação de chaves públicas
- Protocolos de autenticação e estabelecimentos de chaves

Parte II – Autenticação e Autorização

- Autenticação baseada em *passwords*
- Protocolos para gestão distribuída de identidade e autorização
  - Casos de estudo: OpenID Connect, OAuth 2.0
- Modelos, políticas e mecanismos para controlo de acessos
  - Casos de estudo: Listas de controlo de acessos (ACL), Políticas baseadas em papéis (RBAC)

Suporte

Páginas no sistema Moodle	Sumários, Materias de estudo, Enunciados, Entregas
Material de estudo	Conjuntos de slides
	Artigos e manuais
Livros recomendados	D. Gollmann, Computer Security, 3ª edição, Wiley, 2011
	Wenliang Du, Computer Security: A Hands-on Approach, 2ª edição, 2019
Docentes	Diego Passos (diego.passos em isel.pt) Fernanda Passos (fernanda.passos em isel.pt) José Simão (jose.simao em isel.pt) João Vitorino (joao.vitorino em isel.pt)
	Link Zoom anunciado no Moodle

Avaliação

Teste final

- 60% da nota final, nota mínima de 9,5 valores
- A realizar nas datas de exame
- Consulta limitada a 1 folha A4

Dois trabalhos

- 40% da nota final, nota mínima de 9,5 valores
- Apresentação/discussão na semana seguinte à entrega
- Datas previstas
  - Primeiro trabalho: publicação a 20/09/2023; entrega até 25/10/2023
  - Segundo trabalho: publicação a 8/11/2023; entrega até 11/12/2023
  - Realizados em grupos de 2 ou 3 elementos
- Entregas no sistema Moodle

5

VISÃO GERAL

Fundamentos de Segurança

Introdução à Criptografia

6

Fundamentos de Segurança Informática

Segurança: proteção de informação.

Informação, dados, recursos…

Previnir e **detetar** ações não autorizadas.

Três principais **propriedades:**

Confidenciabilidade

Integridade

Disponibilidade

7

Proteção da Informação

Informação e dados estão em:

- Dispositivos de armazenamento;
- **Redes de computadores**.

Proteção pode ser a nível de:

- *Hardware*: dispositivos de processamento, armazenamento, ...
- *Software*: sistema operativo, aplicações, bibliotecas, …
- **Dado**: ficheiros, base de dados, *passwords*, ...
- **Comunicação**: ligações de comunicação local ou de longa distância, *routers*, ...

8

Confidencialidade

Previnir a divulgação não autorizada da informação.

- Esconder conteúdo de utilizadores não autorizados.
- Informação não pode ser vista nem analizada.

Privacidade:

- Inclui meios de garatir quais informações podem ser divulgadas e para quem.

Integridade

Garantia de que informações/dados recebidos estão exatamente como foram enviados por uma entidade autorizada.

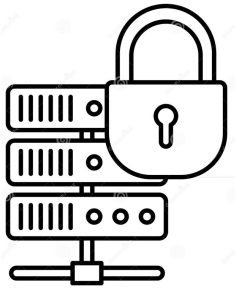
- Conteúdo não pode ser modificado, corrompido ou perdido por terceiros.

Inclui garantir **autenticidade**.

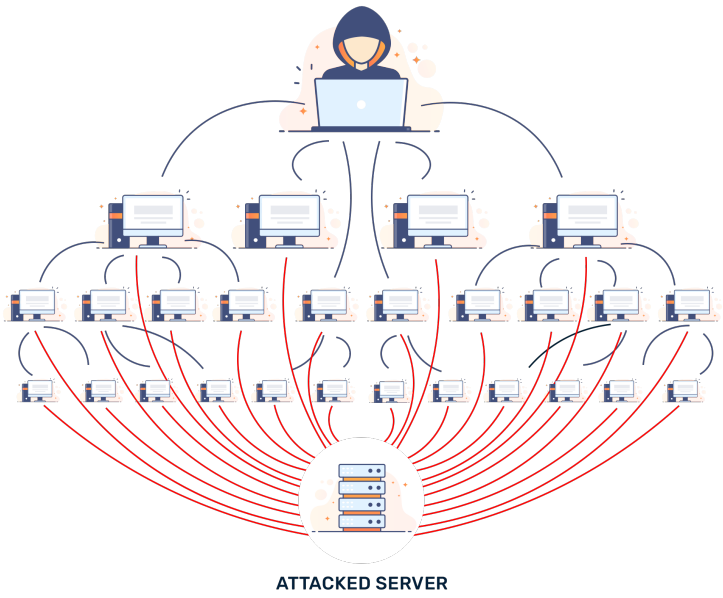
- Isto é, garantir que a entidade envolvida é, de facto, aquela que ela afirma ser.
- Autenticidade muitas vezes é definida como um **quarto princípio**.

Inclui também impedir que entidades neguem a geração da informação.

- **Não-repúdio**.



10



Disponibilidade

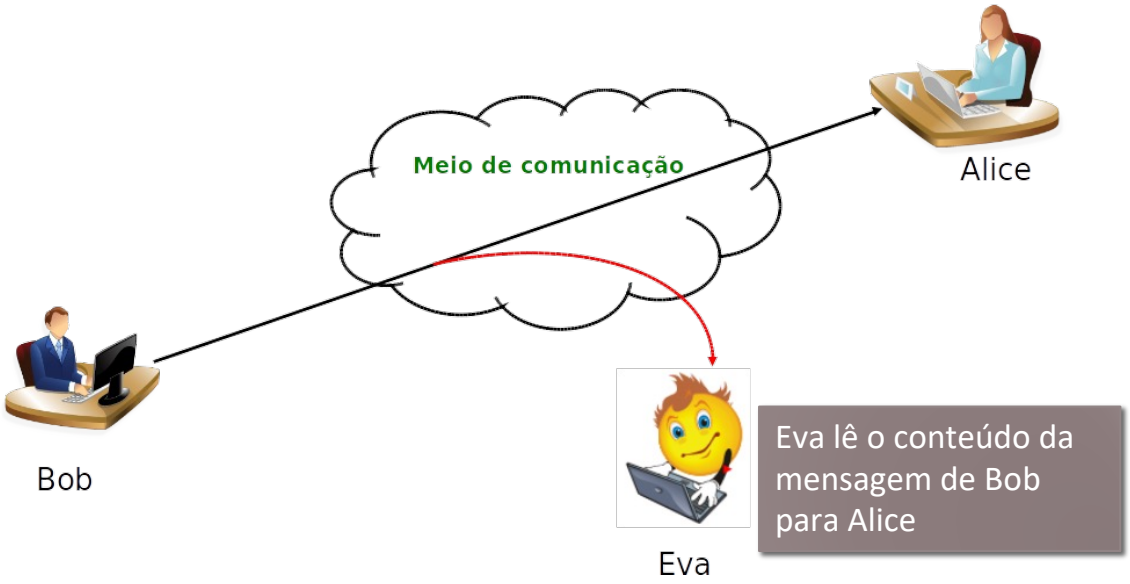
- Propriedade de ser acessível e utilizável sob pedido de uma entidade autorizada.
- Previnir **negação de serviço**.
  - *Denial of service* (DoS)

DDOS - Distributed Denial of Service

Passivos:	Ativos:
• Divulgação de conteúdo • Análise de tráfego	• Disfarce • Repetição • Modificação de mensagem • Negação de serviço

Exemplos de Ataques

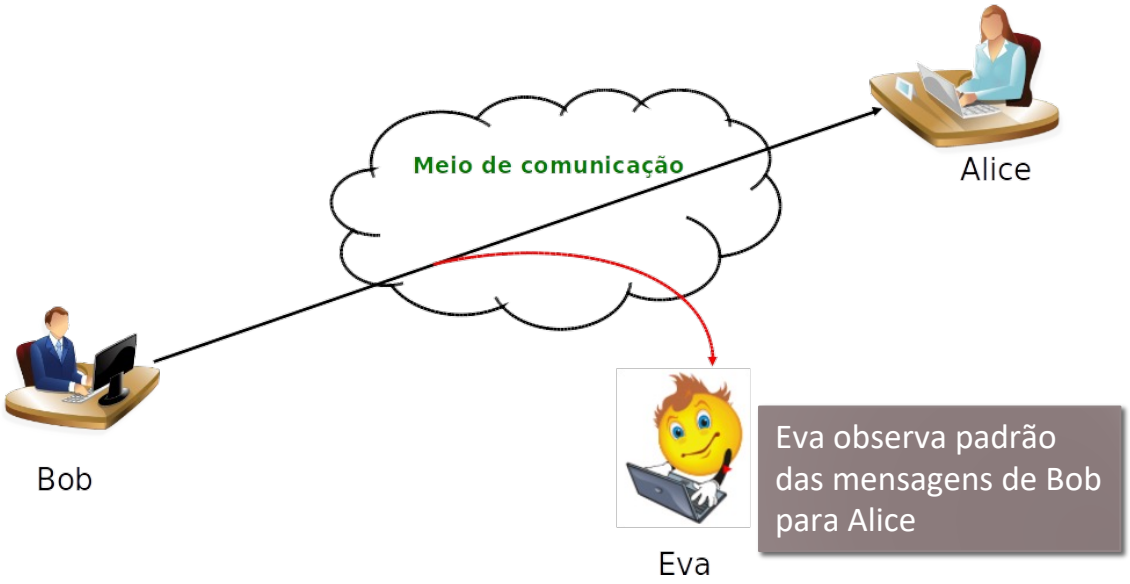
12



Ataque Passivo

DIVULGAÇÃO DE CONTEÚDO

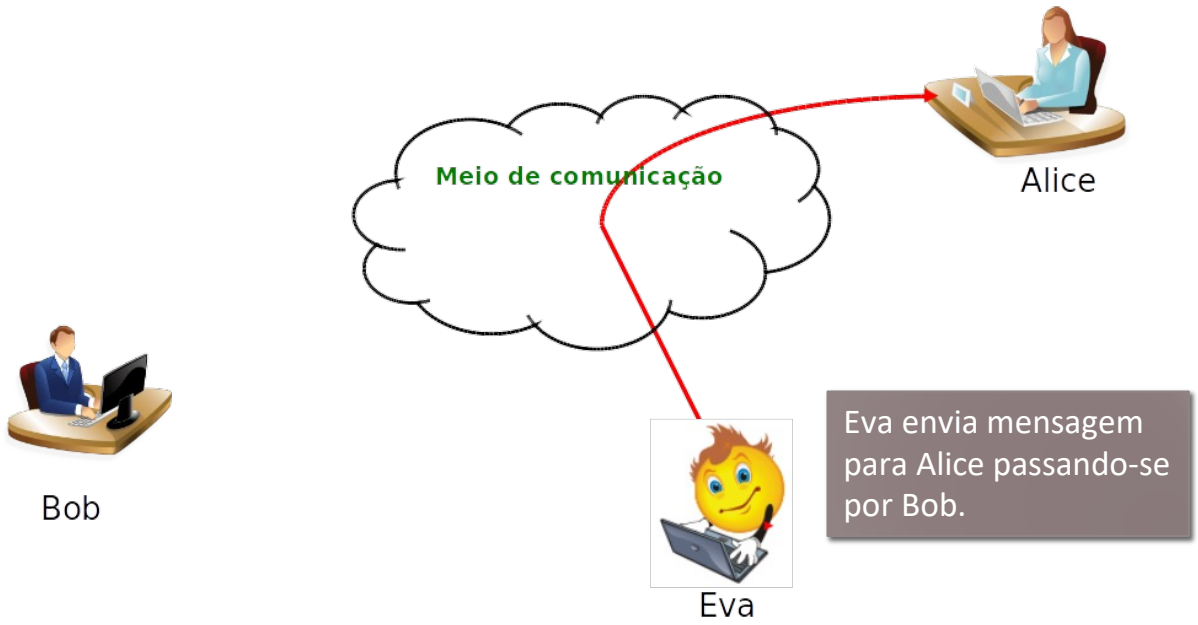
13



Ataque Passivo

ANÁLISE DE TRÁFEGO

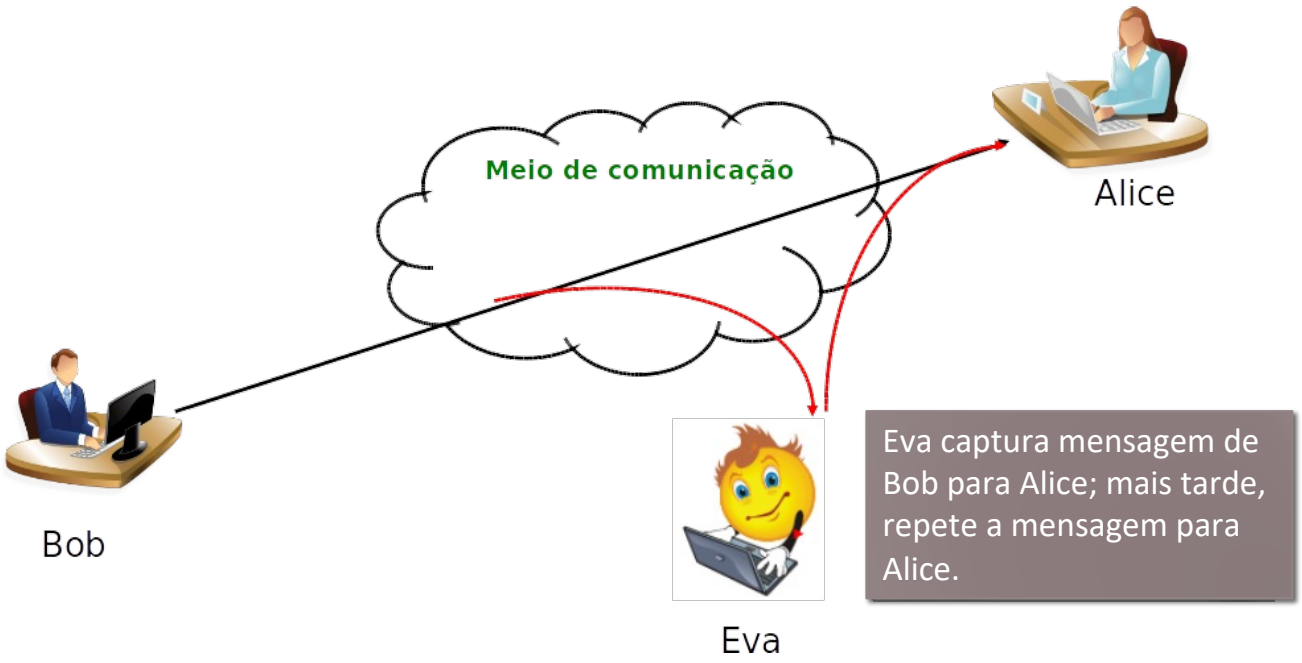
14



Ataque Ativo

DISFARCE

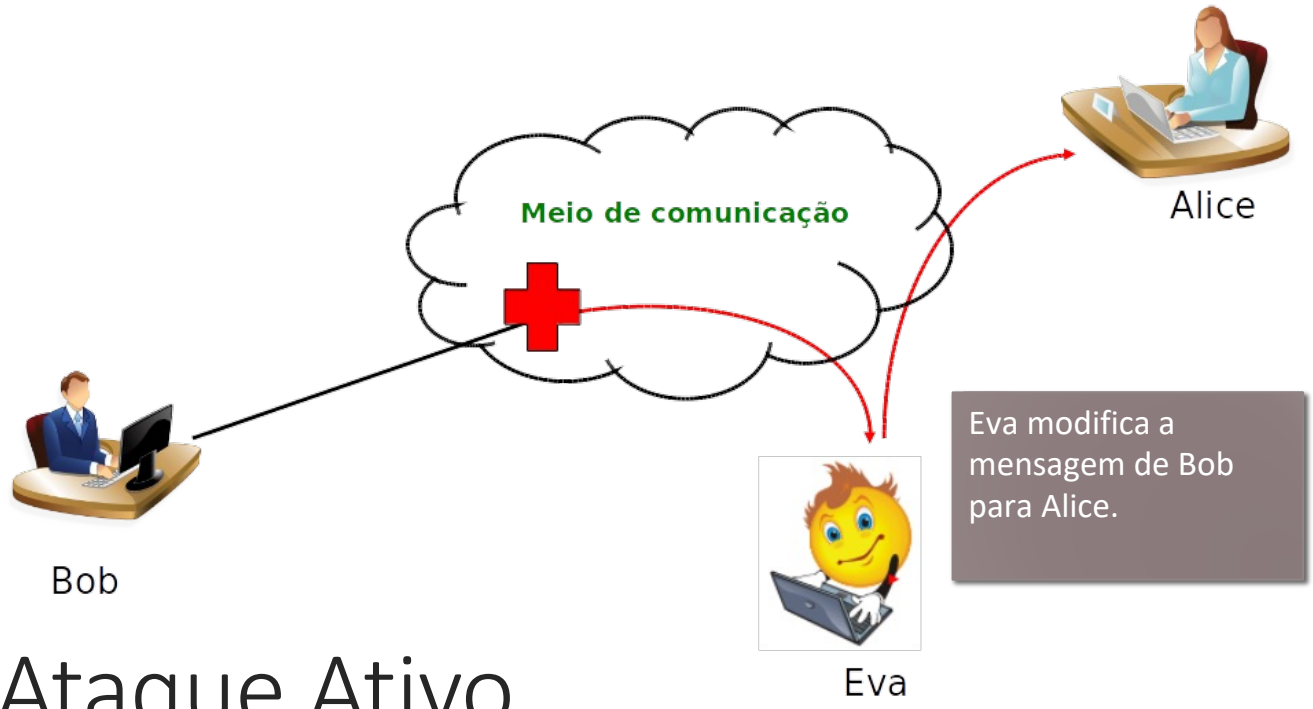
15



Ataque Ativo

REPETIÇÃO

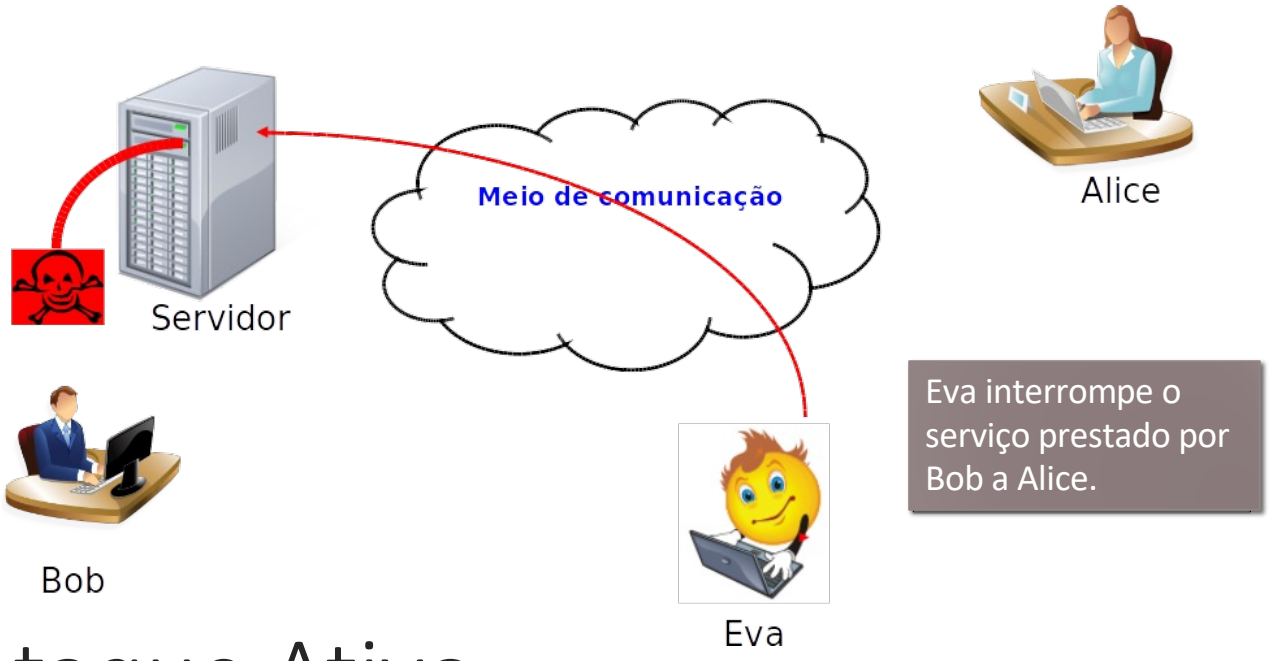
16



Ataque Ativo

MODIFICAÇÃO DE MENSAGEM

17



Ataque Ativo

NEGAÇÃO DE SERVIÇO

18

Introdução à Criptografia

Termos:

- **Criptografia**: ciência de escrever mensagens cifradas.
- **Criptoanálise**: ciência de quebrar códigos e decifrar mensagens.
- **Criptologia**: ciência que reúne criptografia e criptoanálise.

Composição:

- Função de **cifra** (E) que gera criptograma c a partir de mensagem m;
- Função de **decifra** (D) gera m' a partir de c (espera-se m'=m);
- **Chave** (k);
- Função **geradora** de chave (G).

E - função de cifra (encrypt)
D - função de decifra (decrypt)
K - chave (key)
G - função geradora de chave (generator)

Cifra Simples: Cifra de César

A mais antiga cifra de substituição conhecida.

- Utilizada por Júlio César.

Primeiro padrão utilizado em assuntos militares.

Substitui cada letra pela 3ª letra subsequente no alfabeto.

- abcdefgjijklmnopqrstuvwxyz

Exemplo:

TEMOS	UM	EXEMPLO	DE	CIFRA
WHPRV	XP	HAHPSOR	GH	FLIUD

20

Cifra de César: Modelo

Caracteres da mensagem m são mapeados para números de 0 a 25.

- Em ordem alfabética.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Função de geração de chave: G = k = 3

- k é segredo.

Função de cifra: $E(k)(m_i) = (m_i + k)\ mod\ 26 = c_i$

Função de decifra: $D(k)(c_i) = (c_i - k)\ mod\ 26$

21

Criptoanálise da Cifra de César

Apenas 25 possíveis cifras.

- Isto é, k varia de 1 a 25.

Sem saber k, A pode ser mapeado para: A, B, ... , ou Z.

- B será obrigatoriamente pelo próximo símbolo, e assim vai...

Pode-se, simplesmente, tentar um de cada vez.

- Ataque de **força-bruta**.
- Dado texto cifrado, tente todos os deslocamentos possíveis.

É preciso reconhecer o texto plano.

22

Cifra de Substituição Monoalfabética

Ao invés de apenas deslocar o alfabeto, poderia mistura as letras arbitrariamente

Cada letra do texto em claro é mapeada para uma letra cifrada aleatória

Exemplo:

Claro: `abcdefghijklmnopqrstuvwxyz`
Cifrado: `DKVQFIBJWPESCXHTMYAUOLRGZN`

Texto Claro: `ifwewishtoreplaceletters`
Texto Cifrado: `WIRFRWAJUHYFTSDVFSFUUFYA`

Criptoanálise

Agora temos um total de 26! = 4 × 10^{26} chaves.

Com tantas chaves, é um algoritmo seguro?

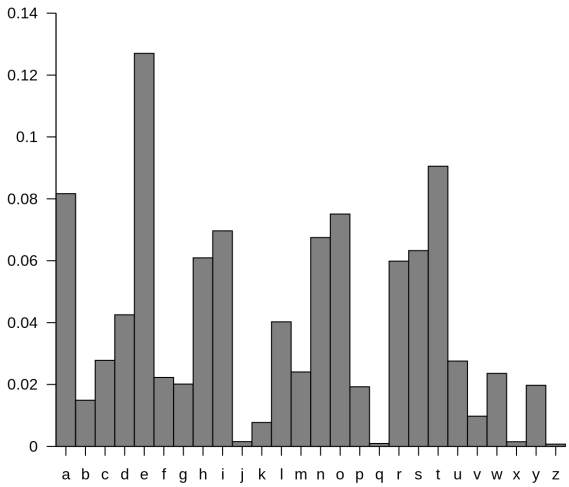
- Errado!!!

Línguas humanas são redundantes.

- Letras não são igualmente usadas.

Letra “E”, em Inglês, é de longe a letra mais comum.

- Seguida por T, A, O, I, N, S, R.
- Outras letras, como Z, Q, X, J, são mais raras.



24

Cifra de Vigenère

É uma cifra de substituição polialfabética.

Uso da seguinte *tabula recta*:

	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
A	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	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	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	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	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
V	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
W	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	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	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
Z	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

Alfabeto de 26 letras.

Chave é subconjunto do alfabeto.

- Exemplo: FRUTA

Alinha-se a chave com a mensagem.

- Repete-se a chave até atingir o comprimento da mensagem.

Mapeia-se as letras de acordo com a tabela.

mapeamento
TEMOSUMEXEMPLODECIFRA
FRUTAFRUTAFRUTAFRUTAF
YVGHSZDYQERGFHDJTCYRF

Experimentar: https://cryptii.com/pipes/vigenere-cipher

25

Cifra de Vigenère: Modelo

Alfabeto é modelado com 26 letras, numeradas de 0 a 25.

- Em ordem alfabética.

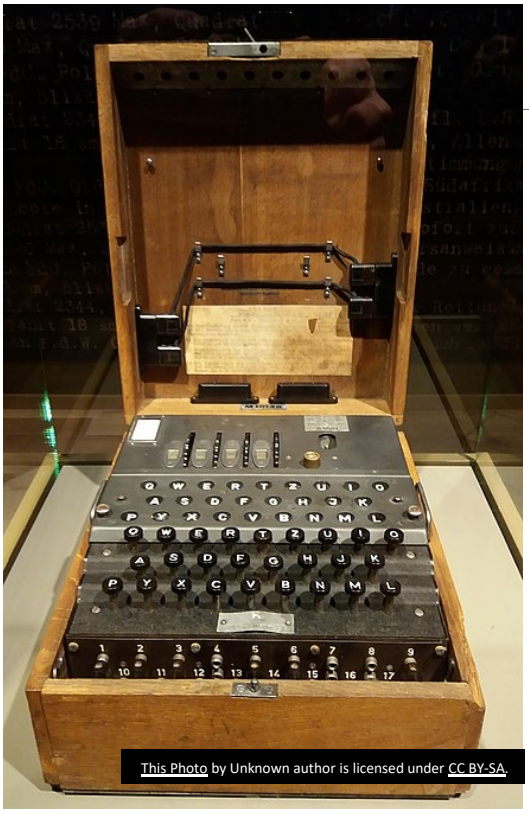
Função de geração de chave: G = k.

- Conjunto de caracteres do alfabeto de tamanho x < n.
- n é o número de caracteres na mensagem m.

Função de cifra: $E(k)(m_i) = (m_i + k_{i \bmod x}) \ mod \ 26 = c_i$

Função de decifra: $D(k)(c_i) = (c_i - k_{i \bmod x}) \ mod \ 26$

26



Máquina Enigma

Máquina utilizada na 2ª Guerra Mundial.

- Alemanha usava-a para cifra e decifra de mensagens sensíveis.
- Formada por teclado, lâmpadas, rotores, ligações eletrônicas, e um painel de tomadas.
- Funcionamento: https://www.youtube.com/watch?v=ybkkiGtJmkM

Cifra de substituição.

- Letra premida é associada a outra letra.
  - *e.g.*, A -> Z e Z -> A.
- Rotores giram a cada cifra, gerando novos padrões de associação.
- Para decifra, deve-se saber posição inicial dos rotores.
  - Trocadas a cada dia, a partir de um livro de códigos trocados a cada mês.

27

Criptoanálise da Enigma

Muito mais complexa que as outras cifras.

- Existem cerca de 10^{20} (100 quintilhões) combinações possíveis.
- Devido às movimentações dos rotores que geram combinações diferentes.

Criptoanálise:

- Conhecimento e acesso a uma máquina igual.
- Uma letra nunca é associada a ela mesma.
- Conhecimento de parte de conteúdo da mensagem:
  - Começava com breve relatório de tempo (ensolarado, chuvoso, …).
  - Terminava com "Heil Hitler".
- Era possível supor combinações de letras (mesmo sem código).
  - Inicialmente por humanos.
  - Depois por máquina Bombe (em 20 minutos), projetada por Alan Turing e Gordon Welchman.
- https://brilliant.org/wiki/enigma-machine/

28