INSTITUTO FEDERAL DE
EDUCAÇÃO CIÊNCIA E
TECNOLOGIA
PARAÍBA

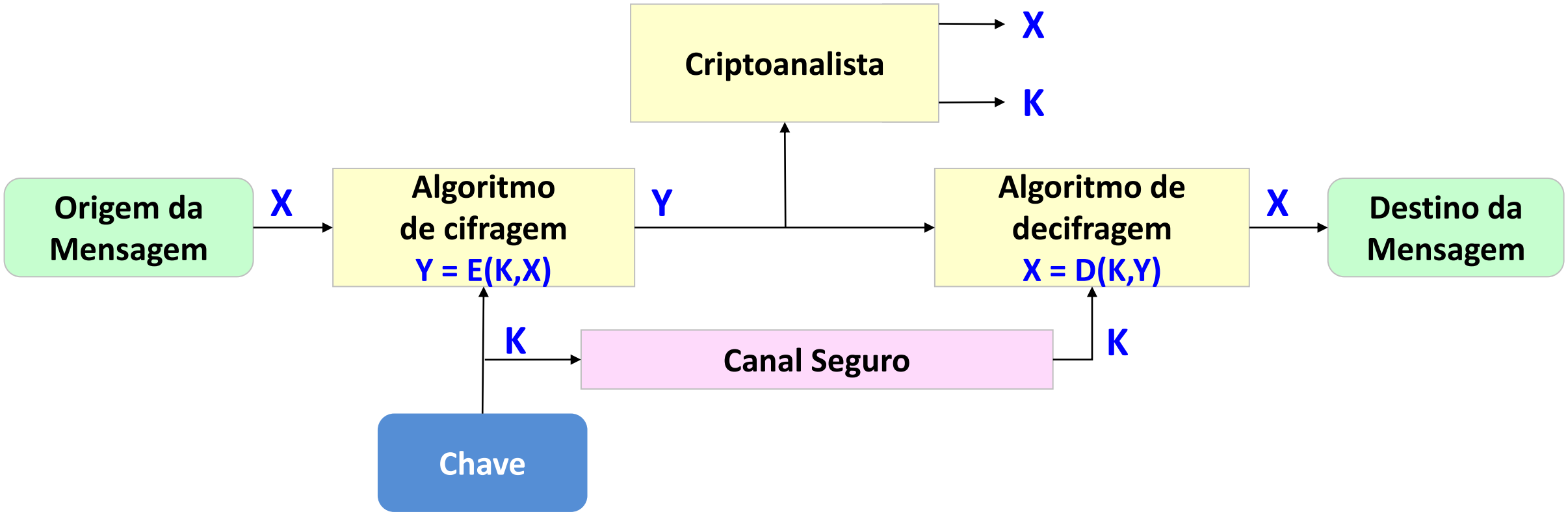
Canal Seguro para Compartilhamento de Chave

Diffie-Hellman Key Exchange

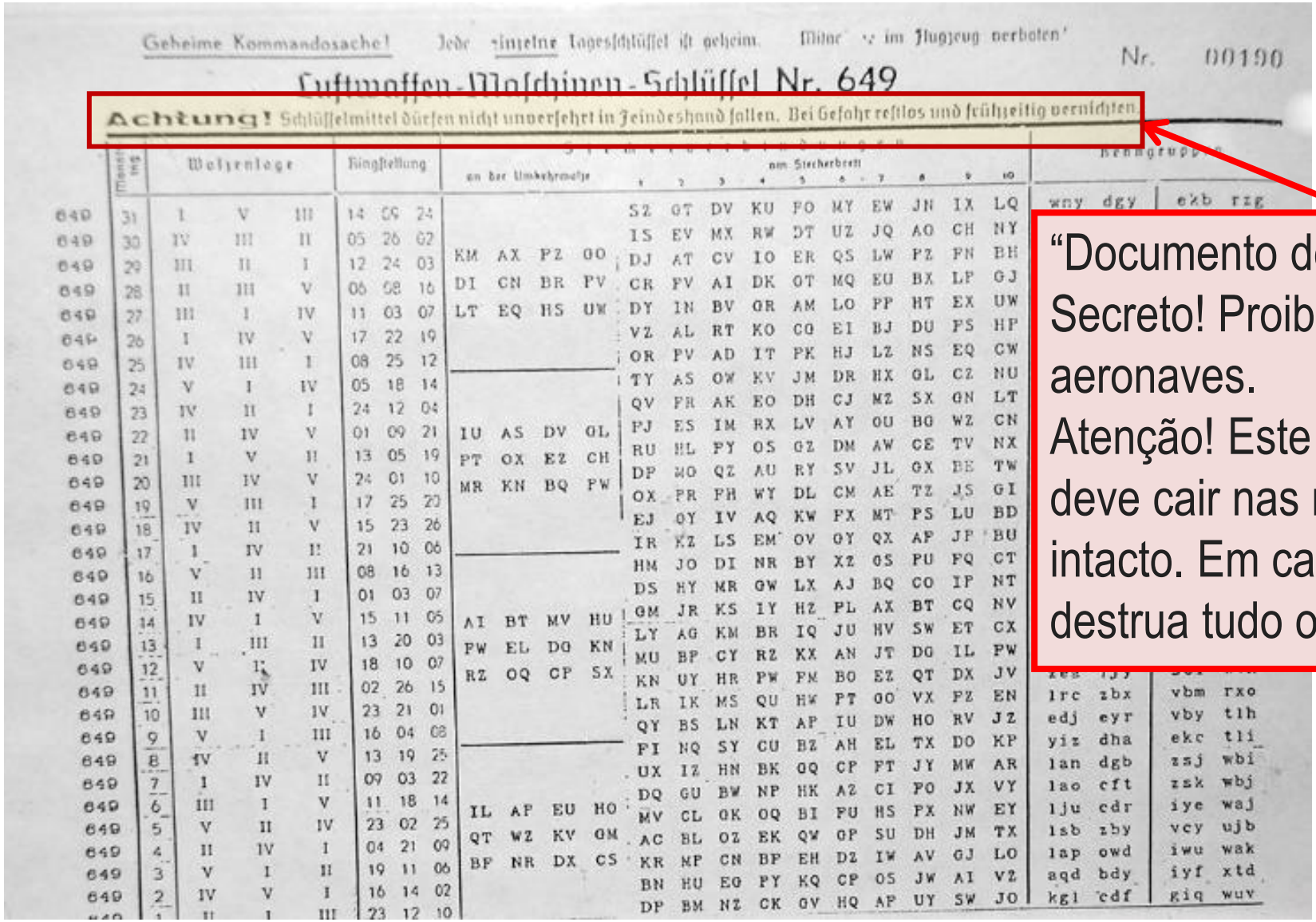
Dênio Mariz
denio@ifpb.edu.br

Fevereiro, 2020

Sistema Criptográfico Simétrico



Problema da troca de chaves


Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitnahme im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

	Monat	Walzenlage			Ringstellung			an der Umkehrwalze				am Steckerbrett										Kenngruppen	
649	31	I	V	III	14	09	24					SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy
649	30	IV	III	II	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY		
649	29	III	II	I	12	24	03	KM	AX	PZ	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH		
649	28	II	III	V	06	08	16	DI	CN	BR	PV	CR	FV	AI	DK	OT	MQ	EU	BX	LP	GJ		
649	27	III	I	IV	11	03	07	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	PP	HT	EX	UW		
649	26	I	IV	V	17	22	19					VZ	AL	RT	KO	CQ	EI	BJ	DU	FS	HP		
649	25	IV	III	I	08	25	12					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	GW		
649	24	V	I	IV	05	18	14					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU		
649	23	IV	II	I	24	12	04					QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT		
649	22	II	IV	V	01	09	21	IU	AS	DV	GL	PJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN		
649	21	I	V	II	13	05	19	PT	OX	EZ	CH	RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX		
649	20	III	IV	V	24	01	10	MR	KN	BQ	PW	DP	WO	QZ	AU	RY	SV	JL	GX	BE	TW		
649	19	V	III	I	17	25	20					OX	PR	PH	WY	DL	CM	AE	TZ	JS	GI		
649	18	IV	II	V	15	23	26					EJ	QY	IV	AQ	KW	FX	MT	PS	LU	BD		
649	17	I	IV	II	21	10	06					IR	KZ	LS	EM	OV	GY	QX	AF	JP	BU		
649	16	V	II	III	08	16	13					HM	JO	DI	NR	BY	XZ	GS	PU	FQ	CT		
649	15	II	IV	I	01	03	07					DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT		
649	14	IV	I	V	15	11	05	AI	BT	MV	HU	GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV		
649	13	I	III	II	13	20	03	FW	EL	DG	KN	LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX		
649	12	V	I	IV	18	10	07	RZ	OQ	CP	SX	MU	BP	CY	RZ	KX	AN	JT	DG	IL	PW		
649	11	II	IV	III	02	26	15					KN	UY	HR	PW	FM	BO	EZ	QT	DX	JV		
649	10	III	V	IV	23	21	01					LR	IK	MS	QU	HW	PT	OO	VX	PZ	EN	lrc	zbx
649	9	V	I	III	16	04	08					QY	BS	LN	KT	AP	IU	DW	HO	RV	JZ	edj	eyr
649	8	IV	II	V	13	19	25					PI	NQ	SY	GU	BZ	AH	EL	TX	DO	KP	yiz	dha
649	7	I	IV	II	09	03	22					UX	IZ	HN	BK	OQ	CP	FT	JY	MW	AR	lan	dgb
649	6	III	I	V	11	18	14	IL	AP	EU	HO	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao	cft
649	5	V	II	IV	23	02	25	QT	WZ	KV	GM	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	lju	cdr
649	4	II	IV	I	04	21	09	BF	NR	DX	CS	AC	BL	OZ	EK	QW	GP	SU	DH	JM	TX	lsb	zby
649	3	V	I	II	19	11	06					KR	MP	CN	BP	EH	DZ	IW	AV	GJ	LO	lap	owd
649	2	IV	V	I	16	14	02					BN	HU	EG	PY	KQ	CP	OS	JW	AI	VZ	aqd	bdy
649	1	II	I	III	23	12	10					DP	BM	NZ	CK	GV	HQ	AP	UY	SW	JO	kgl	cdf

																						vbm	rxo
																						vby	tlh
																						ekc	tli
																						zsj	wbi
																						zsk	wbj
																						iye	waj
																						vcy	ujb
																						iwu	wak
																						iyf	xtd
																						gig	wuv

"Documento de Comando Secreto! Proibido de trazer em aeronaves.
Atenção! Este material chave não deve cair nas mãos do inimigo intacto. Em caso de perigo, destrua tudo o quanto antes"

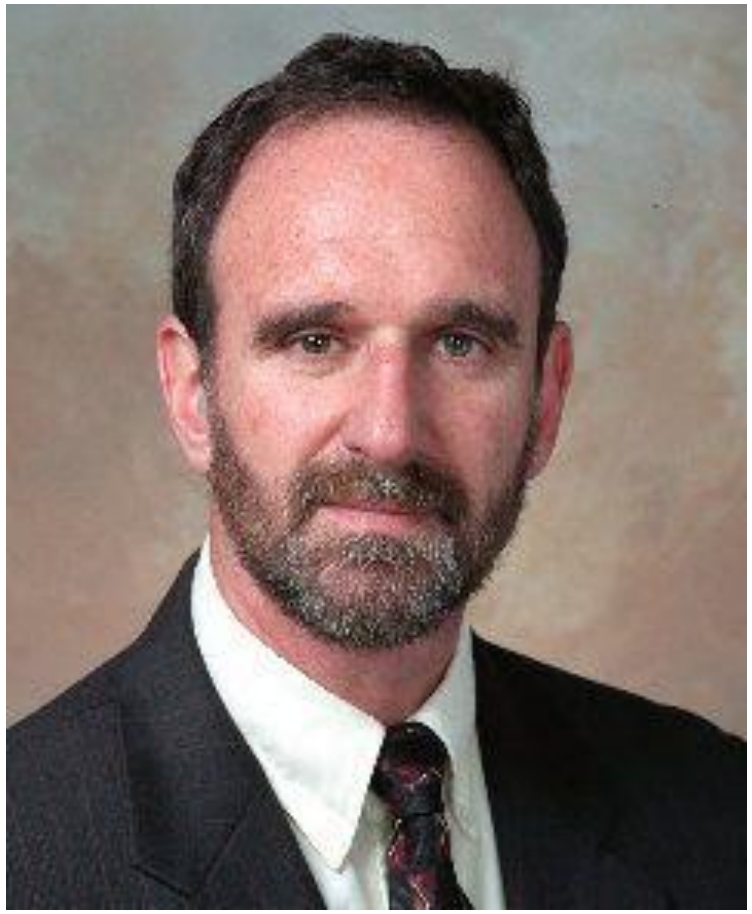
Enigma In Action

https://youtu.be/H8jZ-cXLz70

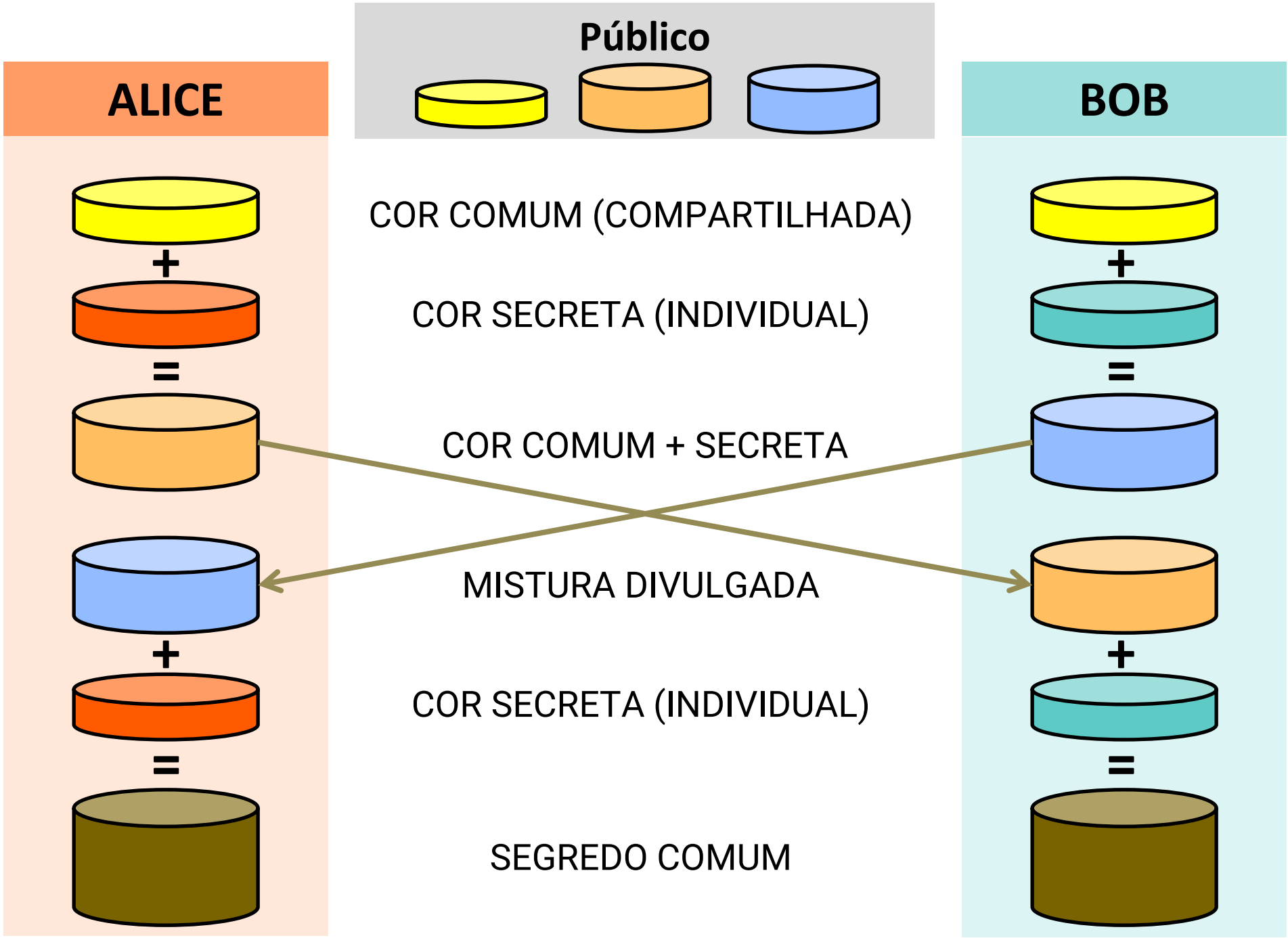
Estabelecendo um Canal Seguro

Diffie-Hellman é um método de criptografia desenvolvido por Whitfield Diffie e Martin Hellman e publicado em 1976.

Whitfield Diffie



Martin Hellman



Fundamentos - Módulo

Propriedade	Exemplo
Associatividade	a + (b + c) mod n = (a + b) + c mod n a * (b * c) mod n = (a * b) * c mod n
Comutatividade	a + b mod n = b + a mod n a * b mod n = b * a mod n
Distributividade	a * (b + c) mod n = ((a * b) + (a * c)) mod n
Redutibilidade	(a + b) mod n = ((a mod n) + (b mod n)) mod n (a * b) mod n = ((a mod n) * (b mod n)) mod n
Potenciação	$a^x \bmod n = (a \bmod n)^x \bmod n$

$a^x \bmod n = (a \bmod n)^x \bmod n$

➔ a=10, x=3, n=7

➔ $(a \bmod n)^x \bmod n = (10 \bmod 7)^3 \bmod 7 =$

$= 3^3 \bmod 7 = 27 \bmod 7 = 6$

➔ $a^x \bmod n = 10^3 \bmod 7 = 1000 \bmod 7 = 6$

Diffie-Hellman Key Exchange

ALICE	ÁREA PÚBLICA	BOB
1. Escolhe um n primo tal que (n-1)/2 também seja primo	→	**<AGUARDA ALICE>**
2. Escolhe g, um gerador módulo n		1. Recebe n, g, a de Alice
3. Escolhe x, um inteiro (segredo)		2. Escolhe um inteiro y (segredo)
4. Calcula **$a=g^x \bmod n$**		3. Calcula **$b=g^y \bmod n$**
5. Envia n, g e a para Bob		4. Envia b para Alice
<AGUARDA BOB>	←	5. Calcula o segredo $s_B=a^y \bmod n$
6. Recebe b de Bob		
7. Calcula o segredo $s_A=b^x \bmod n$		

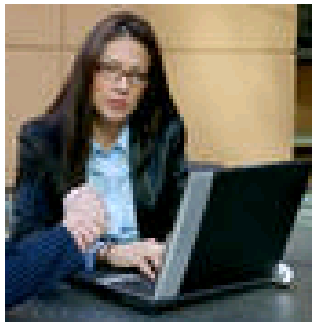
- Se alguém capturar $b=g^y \bmod n$ e $a=g^x \bmod n$ não consegue obter s
- Acredite: $s_A = s_B$ - Portanto, $s_A = s_B = S$ é o segredo compartilhado

Quer dizer que s_A é igual a s_B ?

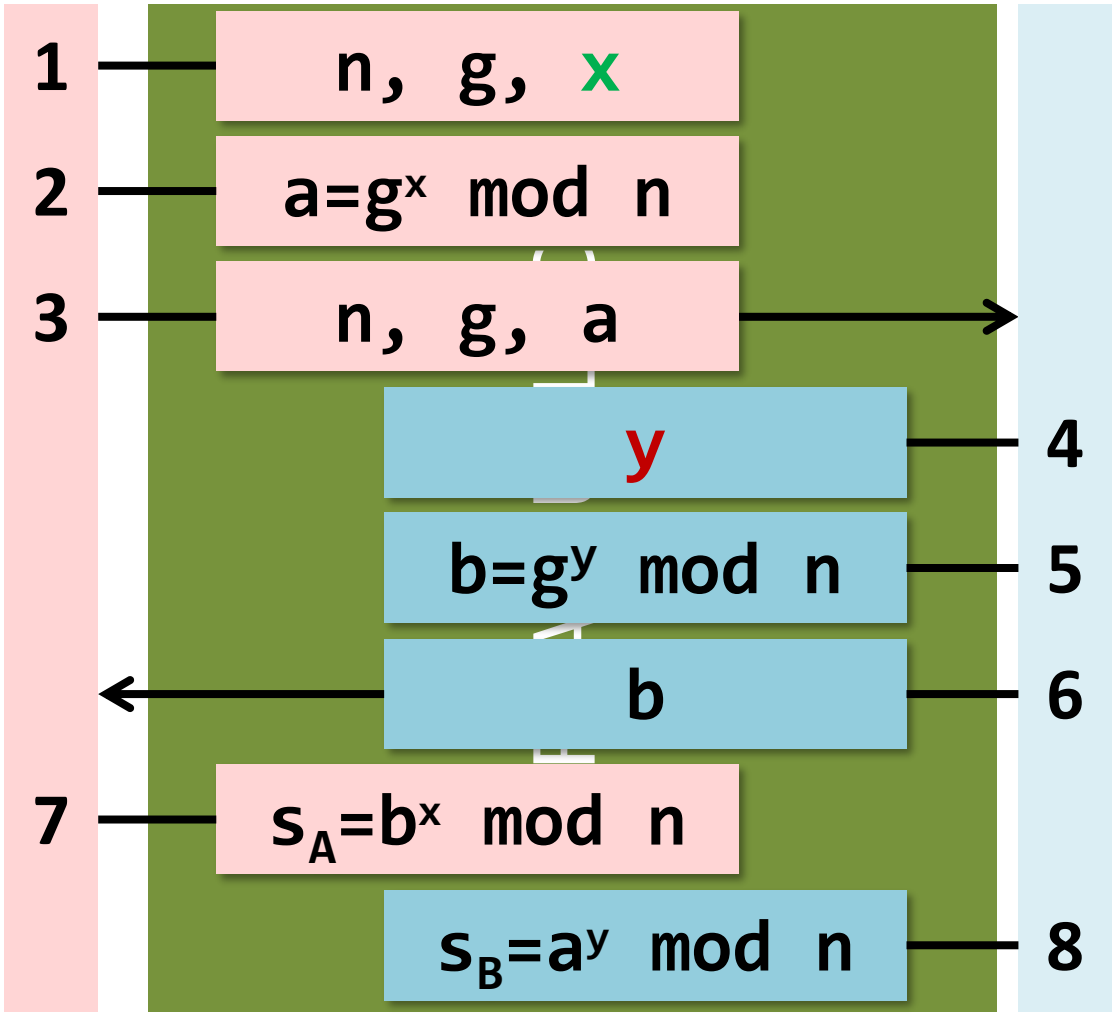
- Lembrar que:
  - $a^x \bmod n = (a \bmod n)^x \bmod n$

- Alice
  - $s_A = b^x \bmod n = (g^y \bmod n)^x \bmod n = \boxed{g^{yx} \bmod n}$
- Bob
  - $s_B = a^y \bmod n = (g^x \bmod n)^y \bmod n = \boxed{g^{xy} \bmod n}$

Diffie-Hellman Key Exchange



Alice



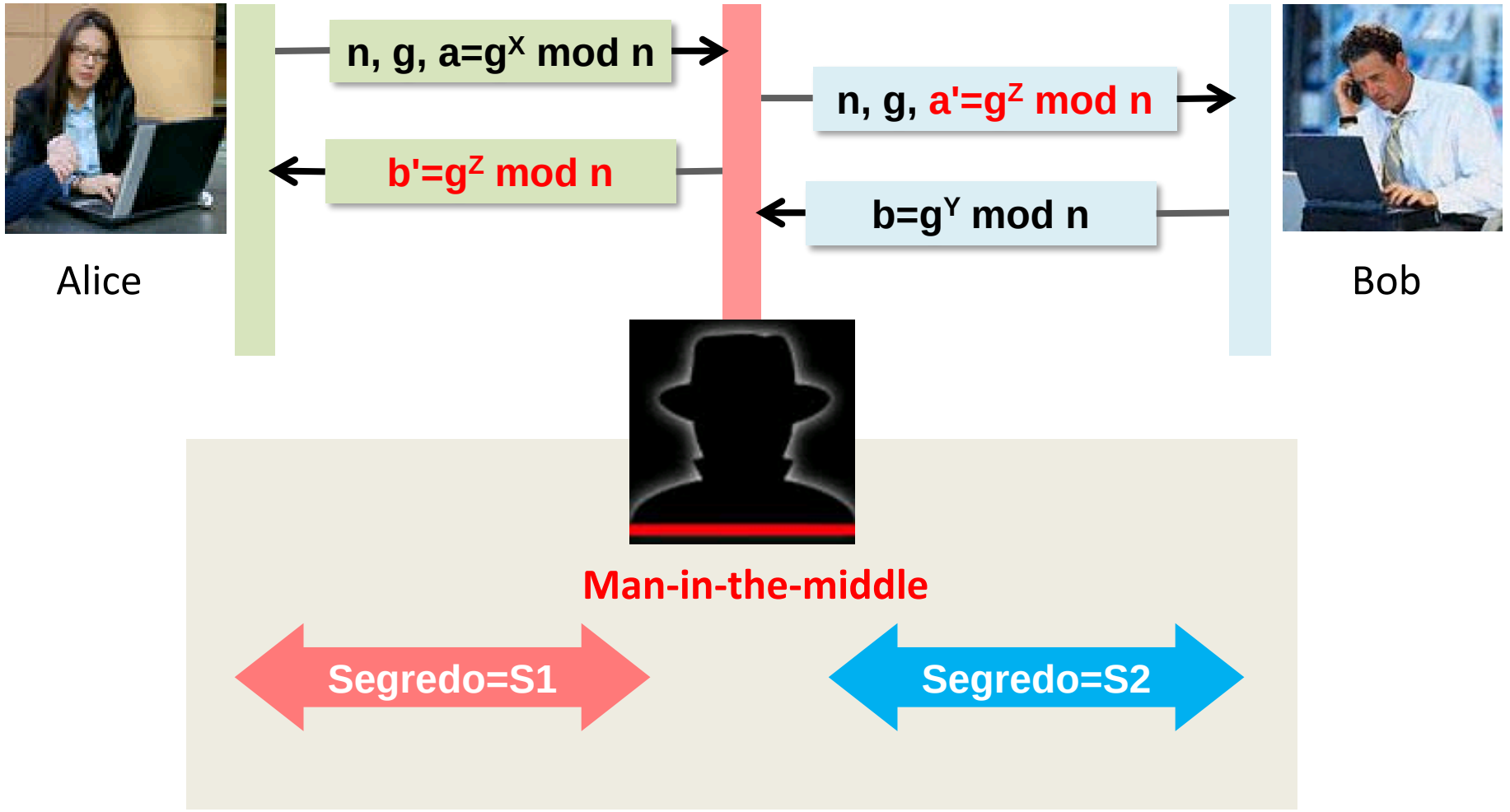
Bob

Diffie-Hellman Key Exchange

➔ Exemplo:

- Alice: n=47, g=3, x=8
- Alice calcula $a=g^x \bmod n = 3^8 \bmod 47 = 28$
- Mensagem de Alice para Bob: {n=47,g=3,a=28}
- Bob pega y=10 e calcula $b=g^y \bmod n = 3^{10} \bmod 47=17$
- Mensagem de Bob para Alice: {b=17}
- Alice calcula $s=b^x \bmod n= 17^8 \bmod 47 = 4$
- Bob calcula $s=a^y \bmod n = 28^{10} \bmod 47 = 4$
- Bob e Alice têm um segredo em comum: s=4
- O segredo pode ser a chave AES 128bits para (cifrar/decifrar)
- Atacante tem que resolver a equação $3^x \bmod 47=28$

Man-in-the-middle Attack



Autenticação baseada em Chave Secreta

- Encontrar x em $g^x \bmod n$ é conhecido como o "Problema do logaritmo discreto"
- Pode levar muito tempo quando g e n são grandes
- Tamanhos típicos para g e n:
  - 512 bits (155 dígitos)
  - Número de 0 até
    13407807929942597099574024998205846127479365820592393377723561443721764030073546976801874298166903427690031858186486050853753882811946569946433649006084095
  - 1024 bits (309 dígitos)
  - Número de 0 até
    179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416624928474306394741243777678934248654852763022196012460941194530829520850057688381506823462462881473913110540827237163350510684586298239947245938479716304835356329624224137215