Criptografía Asimétrica

Miguel Angel Astor Romero

21 de junio de 2019

Agenda

Repaso

Fundamentos de Criptografía Asimétrica

Algoritmo RSA

Aplicaciones

Distribución de Claves

Autenticación de Claves Públicas

Conclusiones

Tipos de cifrado

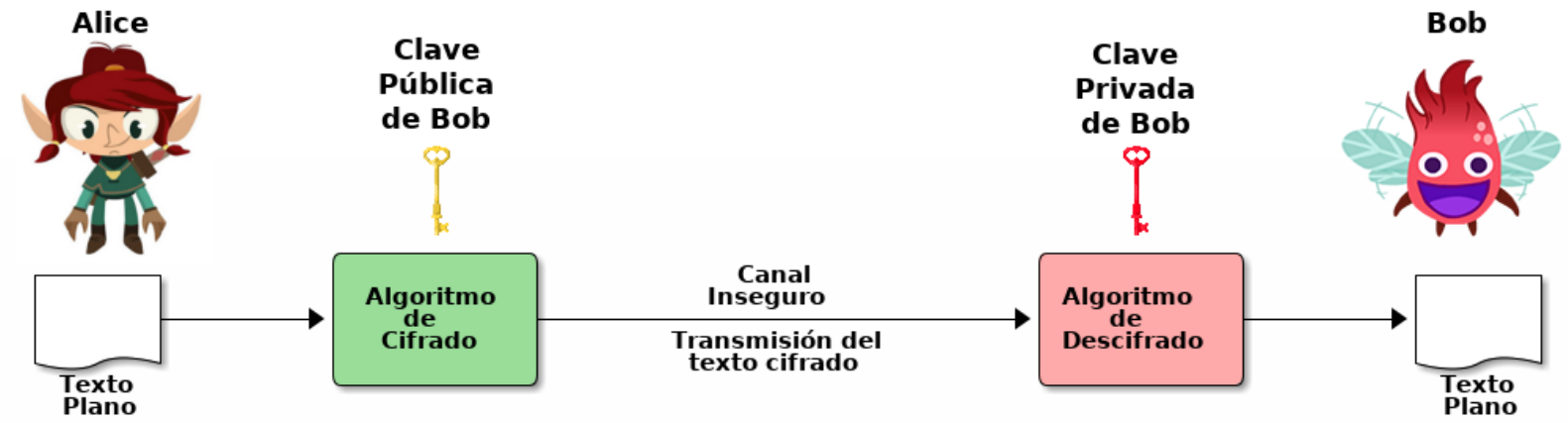
Cifrado simétrico

Conjunto de algoritmos y técnicas de cifrado que utilizan una única clave de cifrado secreta, compartida entre los participantes de la comunicación cifrada.

Cifrado asimétrico

Conjunto de algoritmos y técnicas de cifrado que utiliza dos claves de cifrado: una secreta o privada conocida solo a su dueño, y otra pública conocida por todo el mundo.

Modelo de Criptografía Asimétrica



Bases del Cifrado Asimétrico

El cifrado asimétrico se fundamenta en dos problemas de la aritmética entera:

Factorización Entera

Dado un número compuesto N, hayar sus factores primos.

Logaritmo Discreto

Dados un primo p y una raiz prima a de p, hayar $0 \leq i \leq (p-1)$ tal que

$$b = a^i \text{ mód } p, \quad \forall b \in \mathbb{Z} < p$$

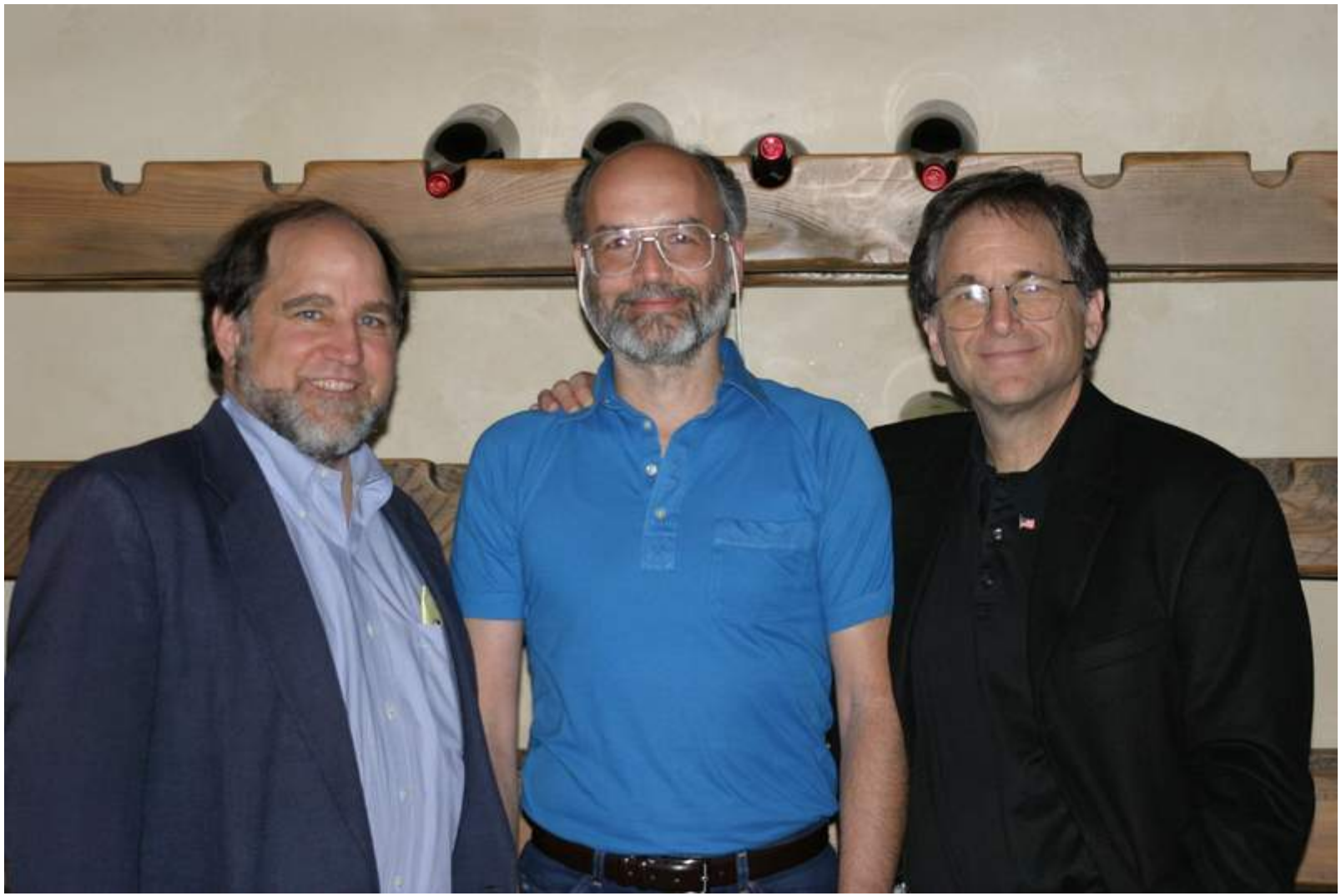
Algoritmos de Cifrado Asimétrico

- RSA
- Elgamal
- Rabin
- DSA
- Cramer-Shoup
- Criptografía de Curva Elíptica

Descripción

- Inventado en 1973 por Clifford Cocks.
- Redescubierto y publicado en 1977 por Rivest, Shamir y Adleman.
- Basado en la dificultad de resolver el problema de factorización entera.

Rivest, Shamir y Adleman



Funcionamiento del Algoritmo

Generación clave

Seleccionar p, q	p y q primos, $p \neq q$
Calcular $n = p \times q$	
Calcular $\phi(n) = (p-1)(q-1)$	
Seleccionar entero e	$gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calcular d	$de \bmod \phi(n) = 1$
Clave pública	$KU = \{e, n\}$
Clave privada	$KR = \{d, n\}$

Cifrado

Texto claro:	$M < n$
Texto cifrado:	$C = M^e \pmod n$

Descifrado

Texto cifrado:	C
Texto claro:	$M = C^d \pmod n$

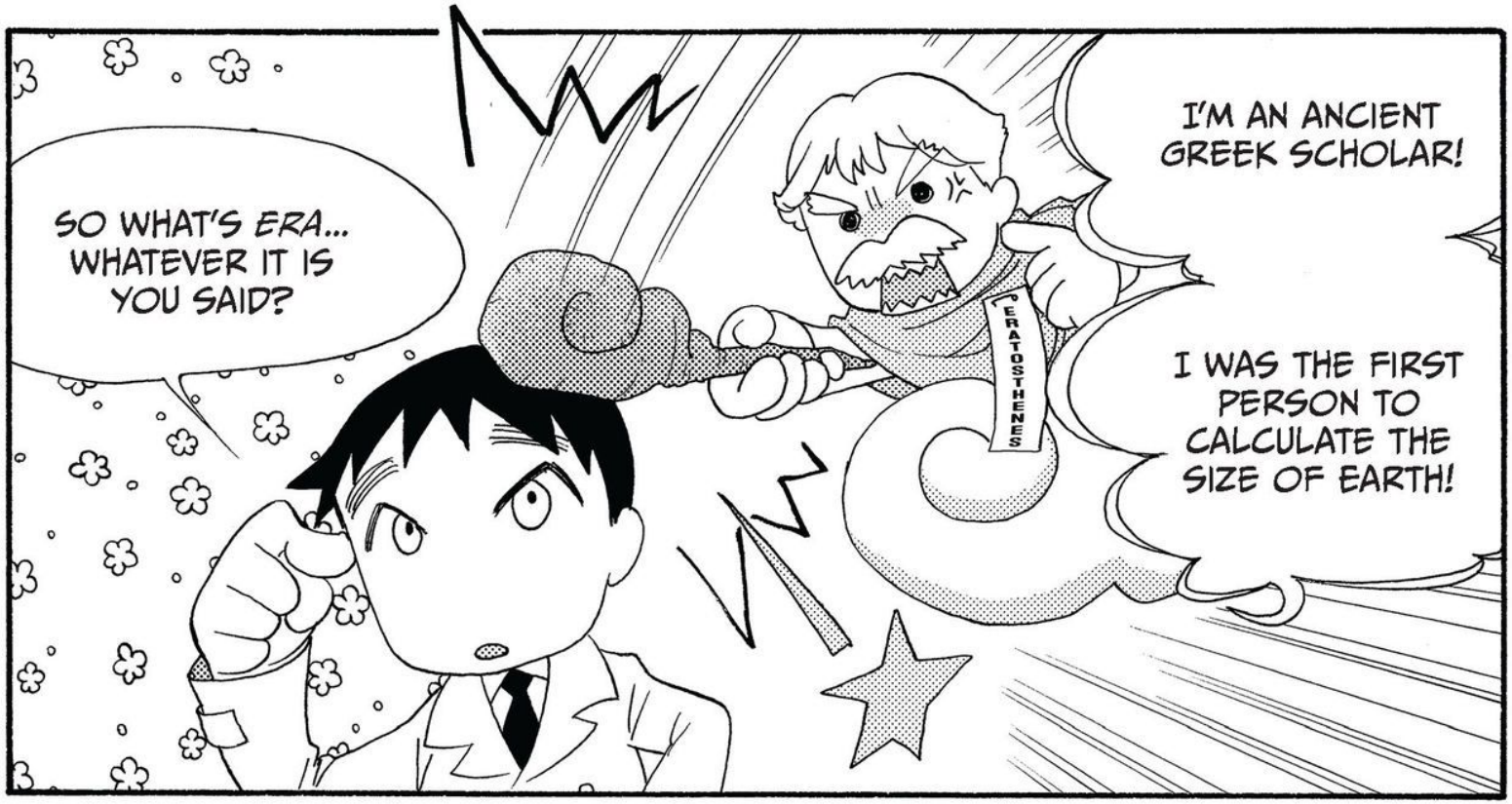
Figura 3.8 El algoritmo RSA

Como Determinar los Números Primos P y Q

Aplicar una prueba de primalidad:

- Criba de Eratóstenes.
- Prueba de Fermat.
- Prueba de Miller–Rabin.
- Prueba de Solovay–Strassen.
- Prueba de Frobenius.

Criba de Eratóstenes



Criba de Eratóstenes - Paso 1

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	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280
281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300
301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320
321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340
341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360
361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380
381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400

Criba de Eratóstenes - Paso 2

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280
281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300
301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320
321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340
341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360
361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380
381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400

Criba de Eratóstenes - Paso 3

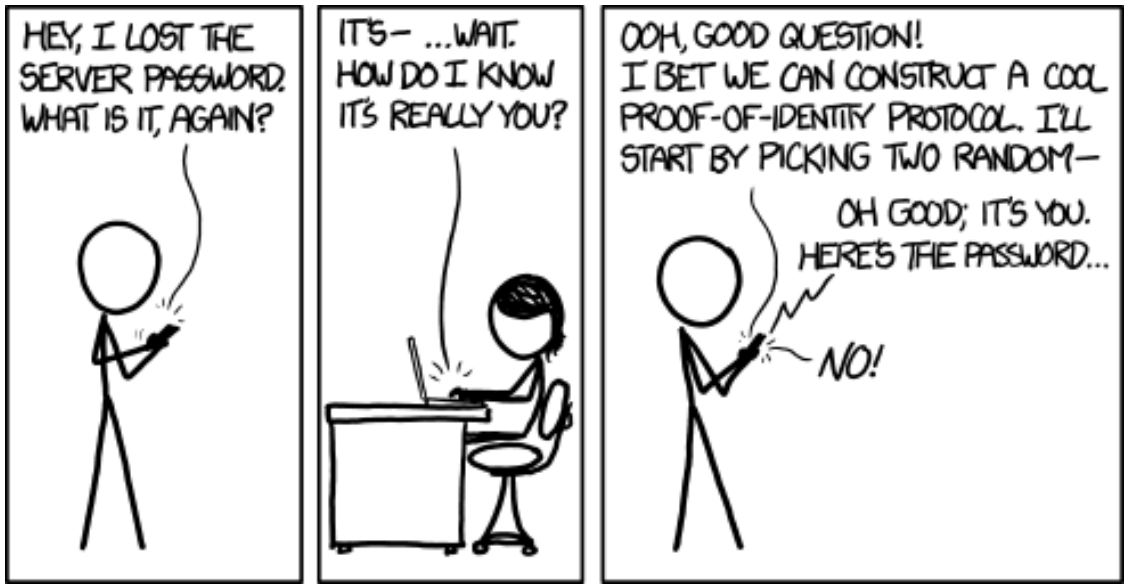
	2	3		5		7		9		11		13		15		17		19	
21		23		25		27		29		31		33		35		37		39	
41		43		45		47		49		51		53		55		57		59	
61		63		65		67		69		71		73		75		77		79	
81		83		85		87		89		91		93		95		97		99	
101		103		105		107		109		111		113		115		117		119	
121		123		125		127		129		131		133		135		137		139	
141		143		145		147		149		151		153		155		157		159	
161		163		165		167		169		171		173		175		177		179	
181		183		185		187		189		191		193		195		197		199	
201		203		205		207		209		211		213		215		217		219	
221		223		225		227		229		231		233		235		237		239	
241		243		245		247		249		251		253		255		257		259	
261		263		265		267		269		271		273		275		277		279	
281		283		285		287		289		291		293		295		297		299	
301		303		305		307		309		311		313		315		317		319	
321		323		325		327		329		331		333		335		337		339	
341		343		345		347		349		351		353		355		357		359	
361		363		365		367		369		371		373		375		377		379	
381		383		385		387		389		391		393		395		397		399	

Criba de Eratóstenes - Paso 4

	2	3		5		7				11		13				17		19	
		23						29		31						37			
41		43				47						53						59	
61						67				71		73						79	
		83						89								97			
101		103				107		109				113							
						127				131						137		139	
								149		151						157			
		163				167						173						179	
181										191		193				197		199	
										211									
		223				227		229				233						239	
241										251						257			
		263						269		271						277			
281		283										293							
						307				311		313				317			
										331						337			
						347		349				353						359	
						367						373						379	
		383						389								397			

Firmas Digitales y no Repudio

Autenticación y Confianza

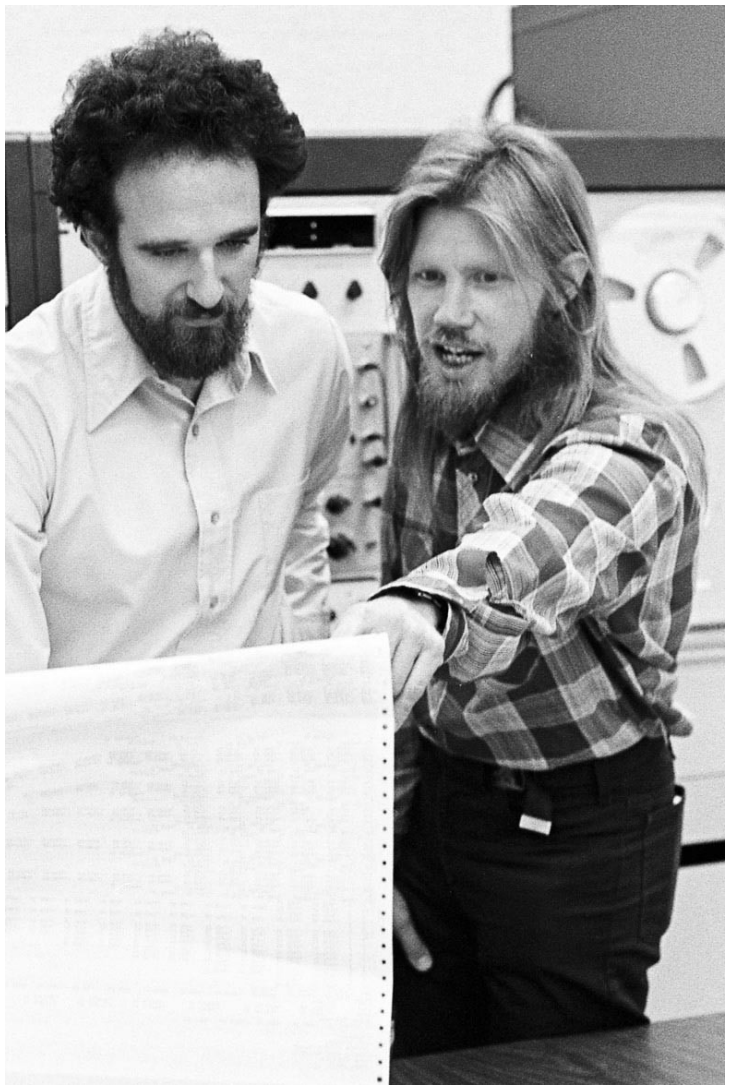


Distribución de Claves

Con el cifrado de clave pública es posible establecer canales seguros para compartir claves simétricas.

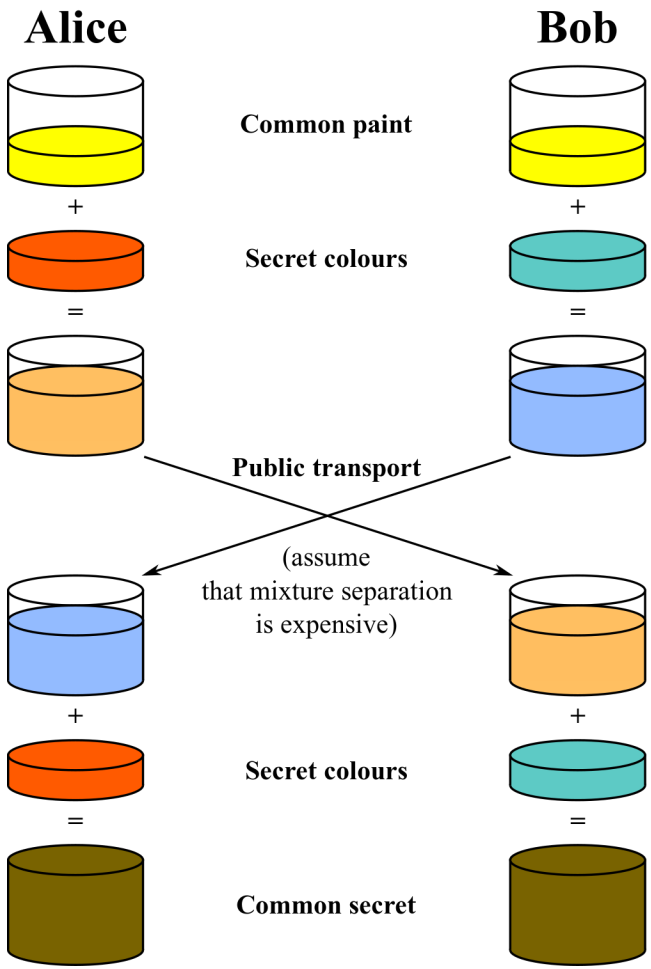
Modelo Completo de Criptografía Simétrica

Algoritmo Diffie-Hellman



- Inventado en 1976 por Whitfield Diffie y Martin Hellman.
- Primer criptosistema de clave pública.
- No usa autenticación.
- Definido para dos participantes, pero generalizable a N participantes.

Funcionamiento general de Diffie-Hellman



- Alice y Bob escogen un color inicial común.
- Luego escogen colores secretos.
- El color público y secreto se mezclan y el resultado se comparte.
- Finalmente se vuelve a mezclar el color secreto con la mezcla del contrario para obtener la clave de sesión.

Una vez más, con números

Elementos públicos globales

q	número primo
α	$\alpha < q$ y α una raíz prima de q

Generación de la clave del usuario *A*

Seleccionar X_A privada	$X_A < q$
Calcular Y_A pública	$Y_A = \alpha^{X_A} \bmod q$

Generación de la clave del usuario *B*

Seleccionar X_B privada	$X_B < q$
Calcular Y_B pública	$Y_B = \alpha^{X_B} \bmod q$

Generación de la clave secreta por el usuario *A*

$K = (Y_B)^{X_A} \bmod q$

Generación de la clave secreta por el usuario *B*

$K = (Y_A)^{X_B} \bmod q$

Figura 3.10 Algoritmo de intercambio de claves de Diffie-Hellman

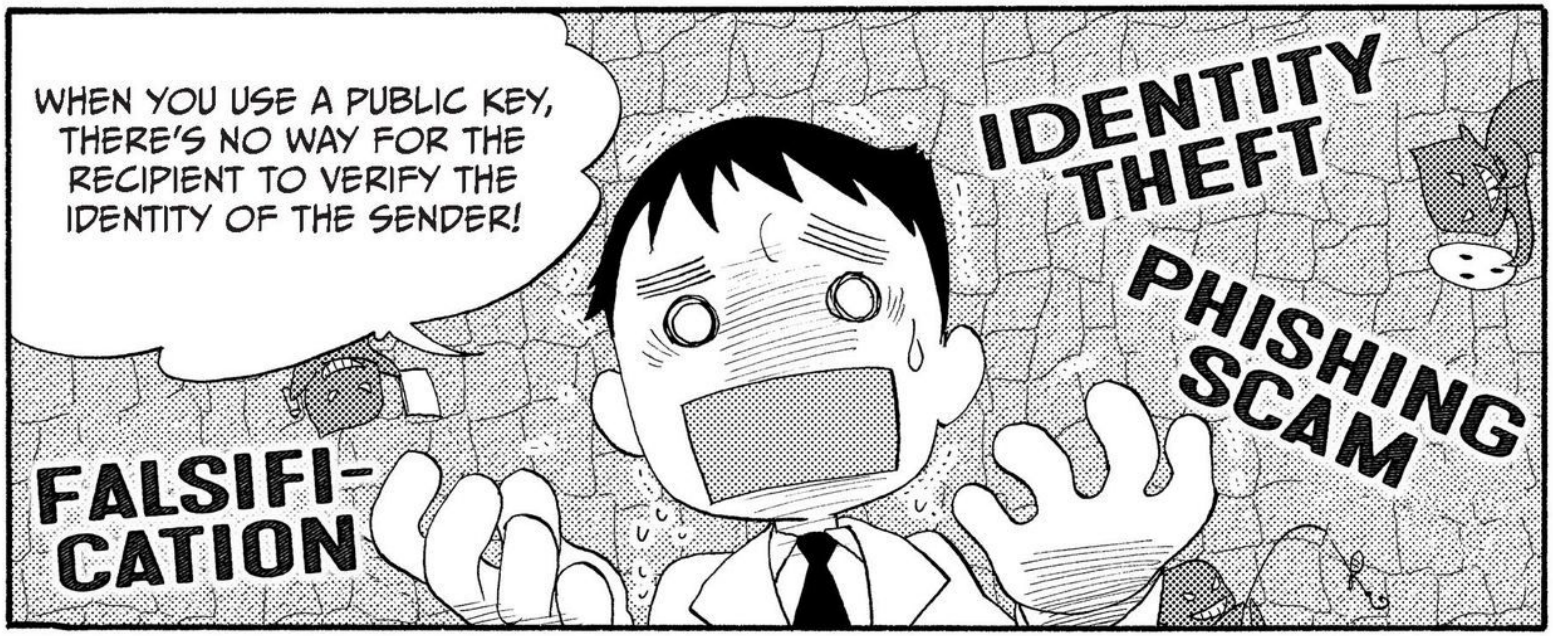
Problema del Logaritmo Discreto

Dado un número primo p y una raiz prima a de p, cualquier entero $b < p$ se puede definir como:

$$b = a^i \text{ mód } p, \quad \text{para } 0 \leq i \leq (p-1)$$

El exponente i se conoce como logaritmo discreto de b para la base a mód p. El algoritmo Diffie-Hellman se fundamenta en el hecho de que i es muy dificil de calcular dados a y p.

El Problema de la Confianza



Soluciones

Vamos a plantear dos posibles soluciones.

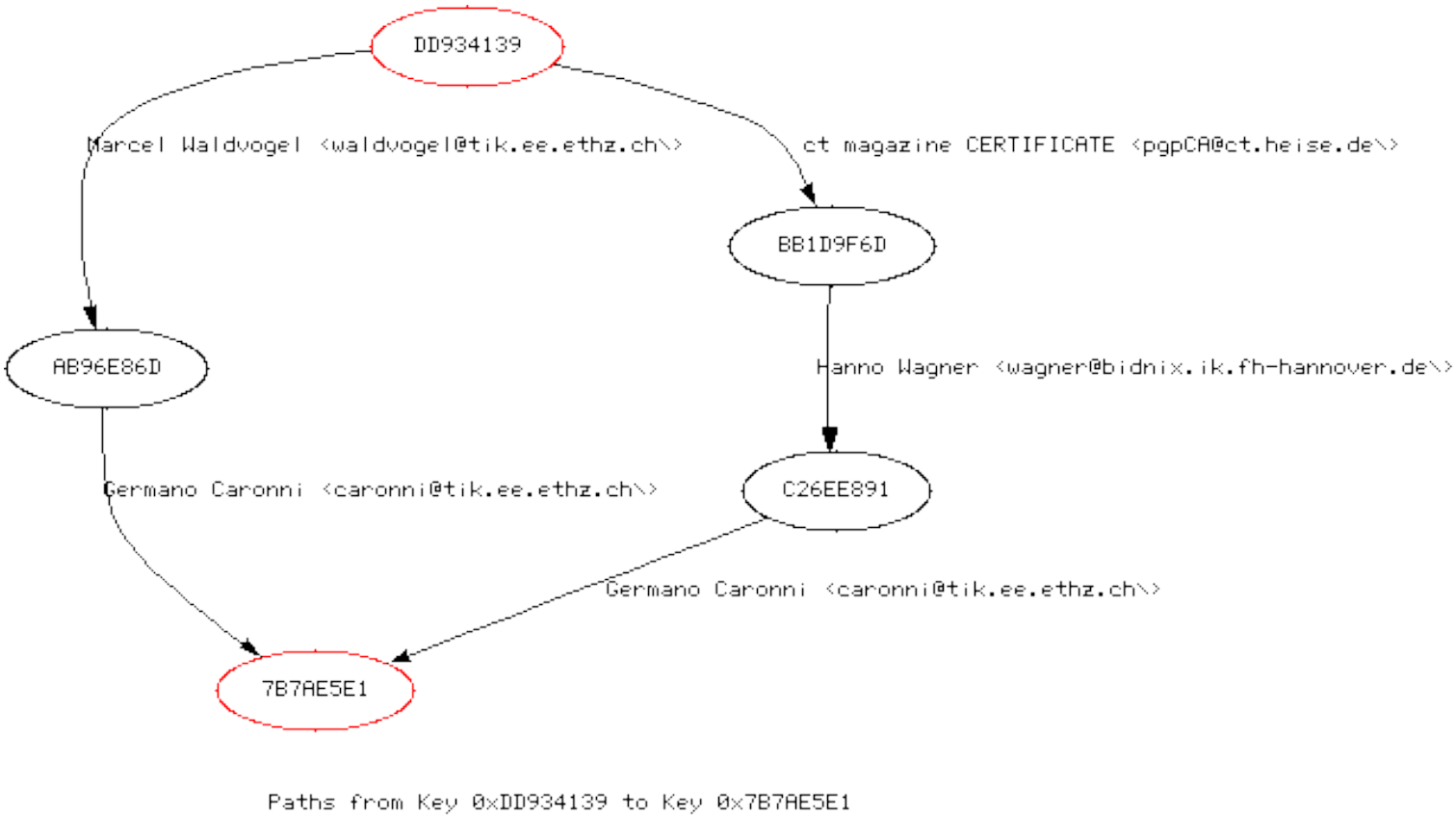
Centralizada

- Utilizar un tercero confiable que verifique la identidad del dueño de una clave pública.
- Norma ITU-T X.509.

Descentralizada

- Utilizar firmas digitales para crear redes de confianza entre usuarios sin un tercero confiable.
- *Web of Trust* en el protocolo OpenPGP (RFC 4880).

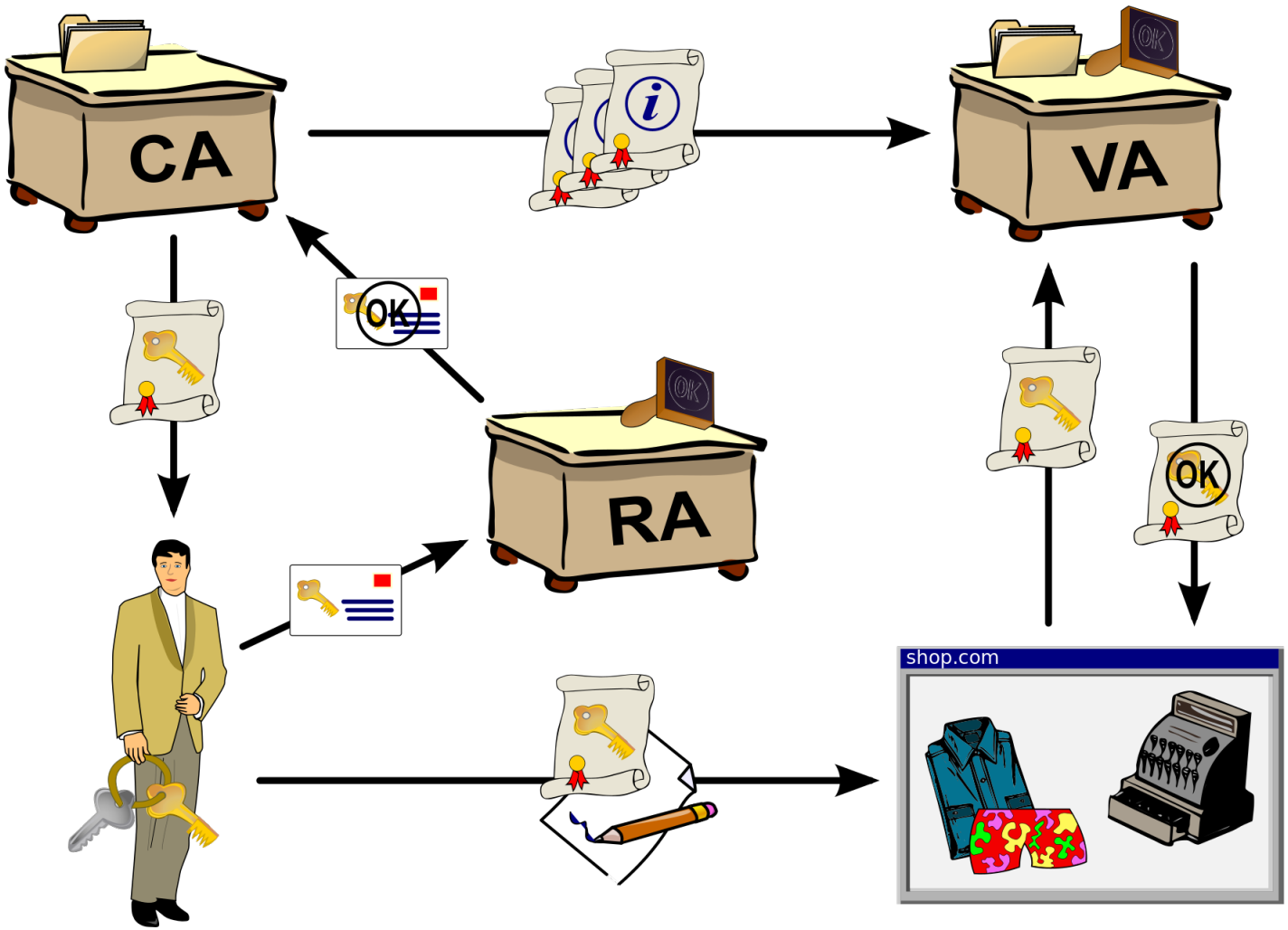
Red de Confianza



Paths from Key 0xDD934139 to Key 0x7B7AE5E1

Problemas con la Red de Confianza

Infraestructura de Clave Pública (PKI)



Conclusiones

- El cifrado asimétrico es fundamentalmente diferente del cifrado simétrico.
- Los algoritmos de clave pública son conceptualmente sencillos, pero involucran problemas difíciles de resolver.
- El cifrado de clave pública tiene muchas aplicaciones más allá del cifrado de mensajes.

Tarea

1. Leer el artículo *"Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice"* y hacer un resumen de máximo 2 páginas de su contenido.

   Fecha de entrega 28 de junio de 2019.

2. Leer el RFC 4880 y hacer un resumen de máxmimo 10 páginas de su contenido.

   Fecha de entrega 12 de julio de 2019.

Las entregas deben hacerse por la sección de entregas del portal de la materia en Portalasig2.

Próxima Clase

- Autenticación:
  - Requerimientos.
  - Códigos de autenticación de mensajes.
  - Funciones *Hash*.
  - Cadenas de Bloques.
  - Firmas digitales.

¿Preguntas?