Applied Cryptograhy

Søren Debois
Februar 20, 2017

Lecture 4

SECURITY F2017

Meta

“The web”

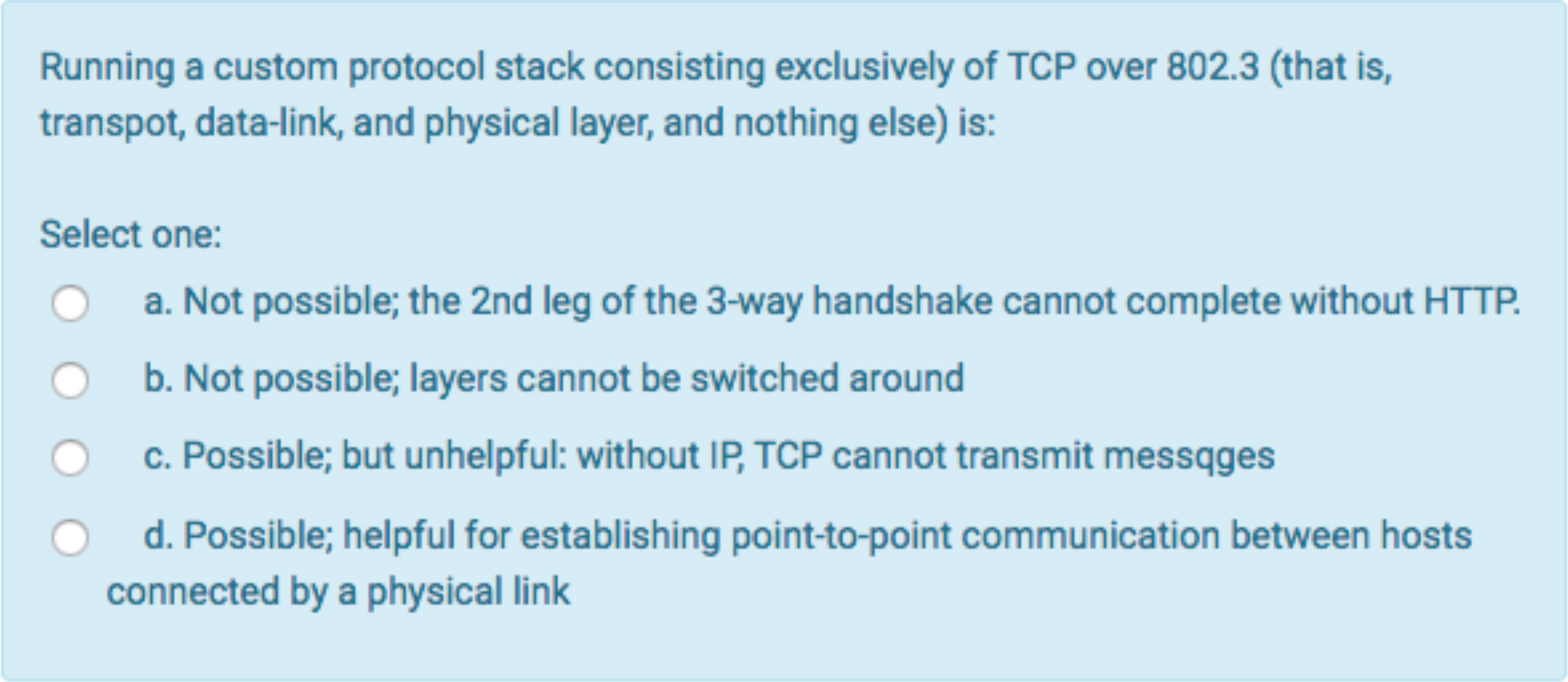
- Peergrade hand-in
- Ok, submission/feedback rates
- However, 3 of you should still be ashamed!
- Generally good solutions :)

learnit quizzes

- Waiting to hear on quiz grade results.
- Look for score of 8.0 or better.
- You will be contacted if you're missing a Quiz.

Quiz results

- Computer networks quiz: Very good, except:



Running a custom protocol stack consisting exclusively of TCP over 802.3 (that is, transpot, data-link, and physical layer, and nothing else) is:

Select one:

○ a. Not possible; the 2nd leg of the 3-way handshake cannot complete without HTTP.

○ b. Not possible; layers cannot be switched around

○ c. Possible; but unhelpful: without IP, TCP cannot transmit messqges

○ d. Possible; helpful for establishing point-to-point communication between hosts connected by a physical link

- Network Security quiz: Excellent!

Applied Cryptography

Motivation

- Preserve confidentiality: only the intended recipient of a message should be able to read it.
- Preserve integrity: An adversary cannot (undetectedly) tamper with a message.

Plan

- Hashes
- Symmetric cryptography
- Asymmetric cryptography
- Signatures, certificates, SSL/TLS

“A proof is any completely convincing argument”

Errett Bishop, 1973
Schizophrenia in Contemporary Mathematics

Cast

- Alice & Bob, who wants to communicate
- Eve, the **e**avesdropper
- Mallet (Mallory), **m**alicious/in the **m**iddle
- Craig, who **c**racks passwords

Cryptographic Hashes

Hashes, digests

- Hash function: Function taking arbitrary length data (“message”) to fixed-length value (“digest”).

- Used in, e.g., hashing, hash table http://en.wikipedia.org/wiki/File:Cryptographic_Hash_Function.svg s (duh).

- Used in, e.g., verifying integrity.

- Used for storing passwords.

“Barstow”

0DFF D632 A3F0 ED84 7B21 5C6E B18E 8FAC 2AA4 FE40

“Barstov”

E5E8 9BBD B5FD BF6A 84ED C94E 5065 C4FC 2FA2 5B32

“We were somewhere around Barstow”

1D8A A942 BE89 ABBF E452 0B1D FBE0 F6D3 821B 0E2D

Full text of Hunter S. Thompson, Fear and Loathing in Las Vegas (292320 characters).

0B9C 44A3 4876 B7F6 0EE4 BAD7 4D52 1CEF F5C7 D8C2

Message	M
Hash-function	h
Digest	d

$$h(M) = d$$

Cryptographic hash, properties

- Given M, finding h(M) should be *easy.*

- *Pre-image resistance:*
  Given d, finding M s.t. h(M) = d should be *infeasible*

- *Second pre-image resistance:*
  Given M, finding M′ with h(M) = h(M′) should be *infeasible*.

- *Collision resistance:*
  Finding M and M′ with h(M) = h(M′) should be *infeasible.*

Cryptographic hash, properties

Term	In practice	In theory
“Easy”	Fast	Probabilistically in polynomial time
“Infeasible”	Beyond the resources of any conceivable adversary	Not probabilistically in polynomial time

Cryptographic hash, properties

- Given M, finding h(M) should be *easy.*

- *Pre-image resistance:*
  Given d, finding M s.t. h(M) = d should be *infeasible*

- *Second pre-image resistance:*
  Given M, finding M′ with h(M) = h(M′) should be *infeasible*.

- *Collision resistance:*
  Finding M and M′ with h(M) = h(M′) should be *infeasible.*

Nobody proved so.

Implementations

- MD5. Broken ca. 2005. Collisions are easy to find.
- SHA-1. Discovered likely insecure ca. 2005. Used in SSL.
- SHA-2 aka SHA-256 or SHA-512.
  As yet unbroken.

Symmetric Cryptography

Encryption & decryption

- Encryption: function from *secret key* and *plaintext* to *ciphertext*

- Decryption: function from *secret key* and *ciphertext* to *plaintext*.

- Security depends on assumption that decryption is *infeasible* to compute when you don’t know K.

Encryption & decryption

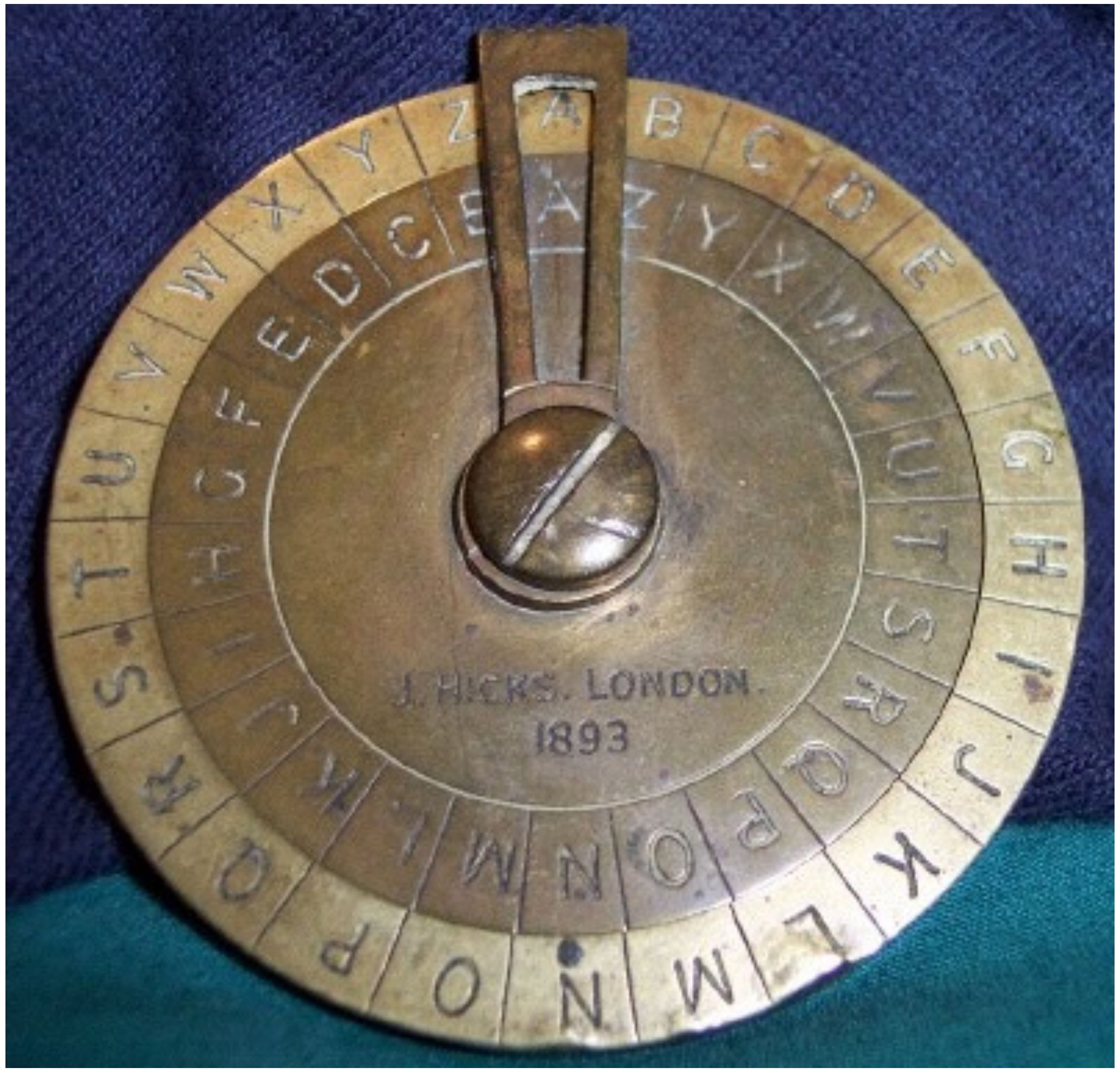
- Encryption: function from *secret key* and *plaintext* to *cipher text*
- Decryption: function from *secret key* and *ciphertext* to *plaintext*.
- Security depends on assumption that decryption is *infeasible* to compute when you don't know K.

DIY

Hello, world!

Caesar-cipher

- Aka “shift cipher”
- Key is rotation of wheel.
- Say, A becomes N.
- Translate A -> N, B -> O, C -> P, …


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 Z Y X W V U T S R Q P O N M L K J I H G F E D C B
J. HICKS. LONDON.
1893

Shift cipher

Key:

ABCDEFGHIKLMNOPQRSTUVWXYZ
NOPQRSTUVXYZABCDEFGHIJKLM

Encryption:

We were somewhere around Barstow
JR JRER FBZRJURER NEBHAQ ONEFGBJ

Shift cipher: Key-space is too small.

```
iq iqdq eayqitqdq mdagzp nmdefai
hp hpcp dzxphspcp lczfyo mlcdezh
go gobo cywogrobo kbyexn lkbcdyg
fn fnan bxvnfqnan jaxdwm kjabcxf
em emzm awumepmzm izwcvl jizabwe
dl dlyl zvtldolyl hyvbuk ihyzavd
ck ckxk yuskcnkxk gxuatj hgxyzuc
bj bjwj xtrjbmjwj fwtzsi gfwxytb
ai aivi wsqialivi evsyrh fevwxsa
zh zhuh vrphzkhuh durxqg eduvwrz
yg ygtg uqogyjgtg ctqwpf dctuvqy
xf xfsf tpnfxifsf bspvoe cbstupx
we were somewhere around barstow
vd vdqd rnldvgdqd zqntmc azqrsnv
uc ucpc qmkcufcpc ypmslb zypqrmu
tb tbob pljbtebob xolrka yxopqlt
sa sana okiasdana wnkqjz xwnopks
rz rzmz njhzrczmz vmjpiy wvmnojr
qy qyly migyqbyly uliohx vulmniq
px pxkx lhfxpaxkx tkhngw utklmhp
ow owjw kgewozwjw sjgmfv tsjklgo
nv nviv jfdvnyviv rifleu srijkfn
mu muhu iecumxuhu qhekdt rqhijem
lt ltgt hdbtlwtgt pgdjcs qpghidl
```

Shift cipher: Key-space is too small

```
iq iqdq eayqitqdq mdagzp nmdefai
hp hpcp dzxphspcp lczfyo mlcdezh
go gobo cywogrobo kbyexn lkbcdyg
fn fnan bxvnfqnan jaxdwm kjabcxf
em emzm awumepmzm izwcvl jizabwe
dl dlyl zvtldolyl hyvbuk ihyzavd
ck ckxk yuskcnkxk gxuatj hgxyzuc
bj bjwj xtrjbmjwj fwtzsi gfwxytb
ai aivi wsqialivi evsyrh fevwxsa
zh zhuh vrphzkhuh durxqg eduvwrz
yg ygtg uqogyjgtg ctqwpf dctuvqy
xf xfsf tpnfxifsf bspvoe cbstupx
we were somewhere around barstow
vd vdqd rnldvgdqd zqntmc azqrsnv
uc ucpc qmkcufcpc ypmslb zypqrmu
tb tbob pljbtebob xolrka yxopqlt
sa sana okiasdana wnkqjz xwnopks
rz rzmz njhzrczmz vmjpiy wvmnojr
qy qyly migyqbyly uliohx vulmniq
px pxkx lhfxpaxkx tkhngw utklmhp
ow owjw kgewozwjw sjgmfv tsjklgo
nv nviv jfdvnyviv rifleu srijkfn
mu muhu iecumxuhu qhekdt rqhijem
lt ltgt hdbtlwtgt pgdjcs qpghidl
```

Arbitrary permutation

- Aka mono-alphabetic substitution

- Instead of simply shifting, pick some random permutation, e.g., A -> Z, B -> C, C -> E, ...

- Very large key-space.
  Number of permutations of letters:
  26! = 26 * 25 * 24 * 23 * 22 * .. * 1 > 4*10^{26}

- Secure?

Mono-alphabetic substitution: Vulnerable to statistical analysis

```
VGUVGOGUZLWGVIGOGUCOLRNFUTCOZQLVULNUQIGUGFHGULBUQIGUFGZGOQUVIGNUQIGF
ORHZUTGHCNUQLUQCYGUILMF3UKUOGWGWTGOUZCXKNHUZLWGQIKNHUMKYGU"KUBGGMUCT
KQUMKHIQIGCFGF;UWCXTGUXLRUZILRMFUFOKSG333U3”UCNFUZRFFGNMXUQIGOGUVCZU
CUQGOOKTMGUOLCOUCMMUCOLRNFURZUCNFUQIGUZYXUVCZUBRMMULBUVICQUMLLYGFUMK
YGUIRHGUTCQZ2UCMMUZVLLJKNHUCNFUZDOGGDIKNHUCNFUFKSKNHUCOLRNFUQIGUDCO2
UVIKDIUVCZUHLKNHUCTLRQUCUIRNFOGFUWKMGZUCNUILROUVKQIUQIGUQLJUFLVNUQLU
MCZUSGHCZ3U …
```

Symbols by frequency:

```
  U G Q C L K N Z I O F M R V D 3 H W X n B T J " 2 Y S   CIPHER
  _ E T A O I N S R H D L U C M F Y W G P B V K X Q J Z   ENGLISH
```

CE CEHE SOWECREHE AHOUND VAHSTOC ON TRE EDYE OB TRE DESEHT CREN TRE
DHUYS VEYAN TO TAJE ROLDF I HEWEWVEH SAGINY SOWETRINY LIJE XI BEEL A
VIT LIYRTREADED; WAGVE GOU SROULD DHIZEF F F FX AND SUDDENLG TREHE
CAS A TEHHIVLE HOAH ALL AHOUND US AND TRE SJG CAS BULL OB CRAT
LOOJED LIJE RUYE VATSQ ALL SCOOKINY AND SMHEEMRINY AND DIZINY AHOUND
TRE MAHQ CRIMR CAS YOINY AVOUT A RUNDHED WILES AN ROUH CITR TRE TOK
DOCN TO LAS ZEYASF

Mono-alphabetic substitution: Vulnerable to statistical analysis

```
VGUVGOGUZLWGVIGOGUCOLRNFUTCOZQLVULNUQIGUGFHGULBUQIGUFGZGOQUVIGNUQIGF
ORHZUTGHCNUQLUQCYGUILMF3UKUOGWGWTGOUZCXKNHUZLWGQIKNHUMKYGU"KUBGGMUCT
KQUMKHIQIGCFGF;UWCXTGUXLRUZILRMFUFOKSG333U3”UCNFUZRFFGNMXUQIGOGUVCZU
CUQGOOKTMGUOLCOUCMMUCOLRNFURZUCNFUQIGUZYXUVCZUBRMMULBUVICQUMLLYGFUMK
YGUIRHGUTCQZ2UCMMUZVLLJKNHUCNFUZDOGGDIKNHUCNFUFKSKNHUCOLRNFUQIGUDCO2
UVIKDIUVCZUHLKNHUCTLRQUCUIRNFOGFUWKMGZUCNUILROUVKQIUQIGUQLJUFLVNUQLU
MCZUSGHCZ3U …
```

Symbols by frequency:

U	G	Q	C	L	K	N	Z	I	O	F	M	R	V	D	3	H	W	X	n	B	T	J	"	2	Y	S	CIPHER
_	E	T	A	O	I	N	S	R	H	D	L	U	C	M	F	Y	W	G	P	B	V	K	X	Q	J	Z	ENGLISH

CE CEHE SOWECREHE AHOUND VAHSTOC ON TRE EDYE OB TRE DESEHT CREN TRE
DHUYS VEYAN TO TAJE ROLDF I HEWEWVEH SAGINY SOWETRINY LIJE XI BEEL A
VIT LIYRTREADED; WAGVE GOU SROULD DHIZEF F F FX AND SUDDENLG TREHE
CAS A TEHHIVLE HOAH ALL AHOUND US AND TRE SJG CAS BULL OB CRAT
LOOJED LIJE RUYE VATSQ ALL SCOOKINY AND SMHEEMRINY AND DIZINY AHOUND
TRE MAHQ CRIMR CAS YOINY AVOUT A RUNDHED WILES AN ROUH CITR TRE TOK
DOCN TO LAS ZEYASF

Most common english trigram: THE

Mono-alphabetic substitution: Vulnerable to statistical analysis

```
VGUVGOGUZLWGVIGOGUCOLRNFUTCOZQLVULNUQIGUGFHGULBUQIGUFGZGOQUVIGNUQIGF
ORHZUTGHCNUQLUQCYGUILMF3UKUOGWGWTGOUZCXKNHUZLWGQIKNHUMKYGU"KUBGGMUCT
KQUMKHIQIGCFGF;UWCXTGUXLRUZILRMFUFOKSG333U3”UCNFUZRFFGNMXUQIGOGUVCZU
CUQGOOKTMGUOLCOUCMMUCOLRNFURZUCNFUQIGUZYXUVCZUBRMMULBUVICQUMLLYGFUMK
YGUIRHGUTCQZ2UCMMUZVLLJKNHUCNFUZDOGGDIKNHUCNFUFKSKNHUCOLRNFUQIGUDCO2
UVIKDIUVCZUHLKNHUCTLRQUCUIRNFOGFUWKMGZUCNUILROUVKQIUQIGUQLJUFLVNUQLU
MCZUSGHCZ3U …
```

Symbols by frequency:

```
  U G Q C L K N Z I O F M R V D 3 H W X n B T J " 2 Y S   CIPHER
  _ E T A O I N S H R D L U C M F Y W G P B V K X Q J Z   ENGLISH
```

CE CERE SOWECHERE AROUND VARSTOC ON THE EDYE OB THE DESERT CHEN THE DRUYS VEYAN TO TAJE HOLDF I REWEWVER SAGINY SOWETHINY LIJE XI BEEL A VIT LIYHTHEADED; WAGVE GOU SHOULD DRIZEF F F FX AND SUDDENLG THERE CAS A TERRIVLE ROAR ALL AROUND US AND THE SJG CAS BULL OB CHAT LOOJED LIJE HUYE VATSQ ALL SCOOKINY AND SMREEMHINY AND DIZINY AROUND THE MARQ CHIMH CAS YOINY AVOUT A HUNDRED WILES AN HOUR CITH THE TOK DOCN TO LAS ZEYASF

Mono-alphabetic substitution: Vulnerable to statistical analysis

```
VGUVGOGUZLWGVIGOGUCOLRNFUTCOZQLVULNUQIGUGFHGULBUQIGUFGZGOQUVIGNUQIGF
ORHZUTGHCNUQLUQCYGUILMF3UKUOGWGWTGOUZCXKNHUZLWGQIKNHUMKYGU"KUBGGMUCT
KQUMKHIQIGCFGF;UWCXTGUXLRUZILRMFUFOKSG333U3”UCNFUZRFFGNMXUQIGOGUVCZU
CUQGOOKTMGUOLCOUCMMUCOLRNFURZUCNFUQIGUZYXUVCZUBRMMULBUVICQUMLLYGFUMK
YGUIRHGUTCQZ2UCMMUZVLLJKNHUCNFUZDOGGDIKNHUCNFUFKSKNHUCOLRNFUQIGUDCO2
UVIKDIUVCZUHLKNHUCTLRQUCUIRNFOGFUWKMGZUCNUILROUVKQIUQIGUQLJUFLVNUQLU
MCZUSGHCZ3U …
```

Symbols by frequency:

```
  U G Q C L K N Z I O F M R V D 3 H W X n B T J " 2 Y S   CIPHER
  _ E T A O I N S H R D L U C M F Y W G P B V K X Q J Z   ENGLISH
```

CE CERE SOWECHERE AROUND VARSTOC ON THE EDYE OB THE DESERT CHEN THE
DRUYS VEYAN TO TAJE HOLDF I REWEWVER SAGINY SOWETHINY LIJE XI BEEL A
VIT LIYHTHEADED; WAGVE GOU SHOULD DRIZEF F F FX AND SUDDENLG THERE
CAS A TERRIVLE ROAR ALL AROUND US AND THE SJG CAS BULL OB CHAT
LOOJED LIJE HUYE VATSQ ALL SCOOKINY AND SMREEMHINY AND DIZINY AROUND
THE MARQ CHIMH CAS YOINY AVOUT A HUNDRED WILES AN HOUR CITH THE TOK
DOCN TO LAS ZEYASF

Long words/phrases with one error.

Mono-alphabetic substitution: Vulnerable to statistical analysis

```
VGUVGOGUZLWGVIGOGUCOLRNFUTCOZQLVULNUQIGUGFHGULBUQIGUFGZGOQUVIGNUQIGF
ORHZUTGHCNUQLUQCYGUILMF3UKUOGWGWTGOUZCXKNHUZLWGQIKNHUMKYGU"KUBGGMUCT
KQUMKHIQIGCFGF;UWCXTGUXLRUZILRMFUFOKSG333U3”UCNFUZRFFGNMXUQIGOGUVCZU
CUQGOOKTMGUOLCOUCMMUCOLRNFURZUCNFUQIGUZYXUVCZUBRMMULBUVICQUMLLYGFUMK
YGUIRHGUTCQZ2UCMMUZVLLJKNHUCNFUZDOGGDIKNHUCNFUFKSKNHUCOLRNFUQIGUDCO2
UVIKDIUVCZUHLKNHUCTLRQUCUIRNFOGFUWKMGZUCNUILROUVKQIUQIGUQLJUFLVNUQLU
MCZUSGHCZ3U …
```

Symbols by frequency:

```
  U G Q C L K N Z I O F M R V D 3 H W X n B T J " 2 Y S   CIPHER
  _ E T A O I N S H R D L U C W F G M Y P V B K X Q J Z   ENGLISH
```

```
CE CERE SOMECHERE AROUND BARSTOC ON THE EDGE OV THE DESERT CHEN THE
DRUGS BEGAN TO TAJE HOLDF I REMEMBER SAYING SOMETHING LIJE XI VEEL A
BIT LIGHTHEADED; MAYBE YOU SHOULD DRIZEF F F FX AND SUDDENLY THERE
CAS A TERRIBLE ROAR ALL AROUND US AND THE SJY CAS VULL OV CHAT
LOOJED LIJE HUGE BATSQ ALL SCOOKING AND SWREEWHING AND DIZING AROUND
THE WARQ CHIWH CAS GOING ABOUT A HUNDRED MILES AN HOUR CITH THE TOK
DOCN TO LAS ZEGASF
```

Mono-alphabetic substitution: Vulnerable to statistical analysis

```
VGUVGOGUZLWGVIGOGUCOLRNFUTCOZQLVULNUQIGUGFHGULBUQIGUFGZGOQUVIGNUQIGF
ORHZUTGHCNUQLUQCYGUILMF3UKUOGWGWTGOUZCXKNHUZLWGQIKNHUMKYGU"KUBGGMUCT
KQUMKHIQIGCFGF;UWCXTGUXLRUZILRMFUFOKSG333U3”UCNFUZRFFGNMXUQIGOGUVCZU
CUQGOOKTMGUOLCOUCMMUCOLRNFURZUCNFUQIGUZYXUVCZUBRMMULBUVICQUMLLYGFUMK
YGUIRHGUTCQZ2UCMMUZVLLJKNHUCNFUZDOGGDIKNHUCNFUFKSKNHUCOLRNFUQIGUDCO2
UVIKDIUVCZUHLKNHUCTLRQUCUIRNFOGFUWKMGZUCNUILROUVKQIUQIGUQLJUFLVNUQLU
MCZUSGHCZ3U …
```

Symbols by frequency:

U	G	Q	C	L	K	N	Z	I	O	F	M	R	V	D	3	H	W	X	n	B	T	J	"	2	Y	S	CIPHER
_	E	T	A	O	I	N	S	H	R	D	L	U	C	W	F	G	M	Y	P	V	B	K	X	Q	J	Z	ENGLISH

CE CERE SOMECHERE AROUND BARSTOC ON THE EDGE OV THE DESERT CHEN THE DRUGS BEGAN TO TAJE HOLDF I REMEMBER SAYING SOMETHING LIJE XI VEEL A BIT LIGHTHEADED; MAYBE YOU SHOULD DRIZEF F F FX AND SUDDENLY THERE CAS A TERRIBLE ROAR ALL AROUND US AND THE SJY CAS VULL OV CHAT LOOJED LIJE HUGE BATSQ ALL SCOOKING AND SWREEWHING AND DIZING AROUND THE WARQ CHIWH CAS GOING ABOUT A HUNDRED MILES AN HOUR CITH THE TOK DOCN TO LAS ZEGASF

Again.

Mono-alphabetic substitution: Vulnerable to statistical analysis

```
VGUVGOGUZLWGVIGOGUCOLRNFUTCOZQLVULNUQIGUGFHGULBUQIGUFGZGOQUVIGNUQIGF
ORHZUTGHCNUQLUQCYGUILMF3UKUOGWGWTGOUZCXKNHUZLWGQIKNHUMKYGU"KUBGGMUCT
KQUMKHIQIGCFGF;UWCXTGUXLRUZILRMFUFOKSG333U3”UCNFUZRFFGNMXUQIGOGUVCZU
CUQGOOKTMGUOLCOUCMMUCOLRNFURZUCNFUQIGUZYXUVCZUBRMMULBUVICQUMLLYGFUMK
YGUIRHGUTCQZ2UCMMUZVLLJKNHUCNFUZDOGGDIKNHUCNFUFKSKNHUCOLRNFUQIGUDCO2
UVIKDIUVCZUHLKNHUCTLRQUCUIRNFOGFUWKMGZUCNUILROUVKQIUQIGUQLJUFLVNUQLU
MCZUSGHCZ3U …
```

Symbols by frequency:

```
  U G Q C L K N Z I O F M R V D 3 H W X n B T J " 2 Y S   CIPHER
  _ E T A O I N S H R D L U W C V G M Y P F B J X Q K Z   ENGLISH
```

```
WE WERE SOMEWHERE AROUND BARSTOW ON THE EDGE OF THE DESERT WHEN THE
DRUGS BEGAN TO TAKE HOLDV I REMEMBER SAYING SOMETHING LIKE XI FEEL A
BIT LIGHTHEADED; MAYBE YOU SHOULD DRIZEV V V VX AND SUDDENLY THERE
WAS A TERRIBLE ROAR ALL AROUND US AND THE SKY WAS FULL OF WHAT
LOOKED LIKE HUGE BATSQ ALL SWOOJING AND SCREECHING AND DIZING AROUND
THE CARQ WHICH WAS GOING ABOUT A HUNDRED MILES AN HOUR WITH THE TOJ
DOWN TO LAS ZEGASV
```

Mono-alphabetic substitution: Vulnerable to statistical analysis

```
VGUVGOGUZLWGVIGOGUCOLRNFUTCOZQLVULNUQIGUGFHGULBUQIGUFGZGOQUVIGNUQIGF
ORHZUTGHCNUQLUQCYGUILMF3UKUOGWGWTGOUZCXKNHUZLWGQIKNHUMKYGU"KUBGGMUCT
KQUMKHIQIGCFGF;UWCXTGUXLRUZILRMFUFOKSG333U3”UCNFUZRFFGNMXUQIGOGUVCZU
CUQGOOKTMGUOLCOUCMMUCOLRNFURZUCNFUQIGUZYXUVCZUBRMMULBUVICQUMLLYGFUMK
YGUIRHGUTCQZ2UCMMUZVLLJKNHUCNFUZDOGGDIKNHUCNFUFKSKNHUCOLRNFUQIGUDCO2
UVIKDIUVCZUHLKNHUCTLRQUCUIRNFOGFUWKMGZUCNUILROUVKQIUQIGUQLJUFLVNUQLU
MCZUSGHCZ3U …
```

Symbols by frequency:

```
  U G Q C L K N Z I O F M R V D 3 H W X n B T J " 2 Y S   CIPHER
  _ E T A O I N S H R D L U W C V G M Y P F B J X Q K Z   ENGLISH
```

WE WERE SOMEWHERE AROUND BARSTOW ON THE EDGE OF THE DESERT WHEN THE DRUGS BEGAN TO TAKE HOLDV I REMEMBER SAYING SOMETHING LIKE XI FEEL A BIT LIGHTHEADED; MAYBE YOU SHOULD DRIZEV V V VX AND SUDDENLY THERE WAS A TERRIBLE ROAR ALL AROUND US AND THE SKY WAS FULL OF WHAT LOOKED LIKE HUGE BATSQ ALL SWOOJING AND SCREECHING AND DIZING AROUND THE CARQ WHICH WAS GOING ABOUT A HUNDRED MILES AN HOUR WITH THE TOJ DOWN TO LAS ZEGASV

Final errors, punctuation.

Mono-alphabetic substitution: Vulnerable to statistical analysis

```
VGUVGOGUZLWGVIGOGUCOLRNFUTCOZQLVULNUQIGUGFHGULBUQIGUFGZGOQUVIGNUQIGF
ORHZUTGHCNUQLUQCYGUILMF3UKUOGWGWTGOUZCXKNHUZLWGQIKNHUMKYGU"KUBGGMUCT
KQUMKHIQIGCFGF;UWCXTGUXLRUZILRMFUFOKSG333U3”UCNFUZRFFGNMXUQIGOGUVCZU
CUQGOOKTMGUOLCOUCMMUCOLRNFURZUCNFUQIGUZYXUVCZUBRMMULBUVICQUMLLYGFUMK
YGUIRHGUTCQZ2UCMMUZVLLJKNHUCNFUZDOGGDIKNHUCNFUFKSKNHUCOLRNFUQIGUDCO2
UVIKDIUVCZUHLKNHUCTLRQUCUIRNFOGFUWKMGZUCNUILROUVKQIUQIGUQLJUFLVNUQLU
MCZUSGHCZ3U …
```

Symbols by frequency:

```
  U G Q C L K N Z I O F M R V D 3 H W X n B T J " 2 Y S   CIPHER
  _ E T A O I N S H R D L U W C . G M Y J F B P "   , K V   ENGLISH
```

```
WE WERE SOMEWHERE AROUND BARSTOW ON THE EDGE OF THE DESERT WHEN THE
DRUGS BEGAN TO TAKE HOLD. I REMEMBER SAYING SOMETHING LIKE "I FEEL A
BIT LIGHTHEADED; MAYBE YOU SHOULD DRIVE. . . ." AND SUDDENLY THERE
WAS A TERRIBLE ROAR ALL AROUND US AND THE SKY WAS FULL OF WHAT
LOOKED LIKE HUGE BATS, ALL SWOOPING AND SCREECHING AND DIVING AROUND
THE CAR, WHICH WAS GOING ABOUT A HUNDRED MILES AN HOUR WITH THE TOP
DOWN TO LAS VEGAS.
```

Broken.

Mono-alphabetic substitution: Vulnerable to statistical analysis

```
VGUVGOGUZLWGVIGOGUCOLRNFUTCOZQLVULNUQIGUGFHGULBUQIGUFGZGOQUVIGNUQIGF
ORHZUTGHCNUQLUQCYGUILMF3UKUOGWGWTGOUZCXKNHUZLWGQIKNHUMKYGU"KUBGGMUCT
KQUMKHIQIGCFGF;UWCXTGUXLRUZILRMFUFOKSG333U3”UCNFUZRFFGNMXUQIGOGUVCZU
CUQGOOKTMGUOLCOUCMMUCOLRNFURZUCNFUQIGUZYXUVCZUBRMMULBUVICQUMLLYGFUMK
YGUIRHGUTCQZ2UCMMUZVLLJKNHUCNFUZDOGGDIKNHUCNFUFKSKNHUCOLRNFUQIGUDCO2
UVIKDIUVCZUHLKNHUCTLRQUCUIRNFOGFUWKMGZUCNUILROUVKQIUQIGUQLJUFLVNUQLU
MCZUSGHCZ3U …
```

Symbols by frequency:

```
  U G Q C L K N Z I O F M R V D 3 H W X n B T J " 2 Y S   CIPHER
  _ E T A O I N S H R D L U W C V G M Y P F B J X Q K Z   ENGLISH
```

```
WE WERE SOMEWHERE AROUND BARSTOW ON THE EDGE OF THE DESERT WHEN THE
DRUGS BEGAN TO TAKE HOLDV I REMEMBER SAYING SOMETHING LIKE XI FEEL A
BIT LIGHTHEADED; MAYBE YOU SHOULD DRIZEV V V VX AND SUDDENLY THERE
WAS A TERRIBLE ROAR ALL AROUND US AND THE SKY WAS FULL OF WHAT
LOOKED LIKE HUGE BATSQ ALL SWOOJING AND SCREECHING AND DIZING AROUND
THE CARQ WHICH WAS GOING ABOUT A HUNDRED MILES AN HOUR WITH THE TOJ
DOWN TO LAS ZEGASV
```

Final errors, punctuation.

Encryption

$E(K,M) = \{M\}_K$

Decryption

$D(K,\{M\}_K) = M$

Theorem

$D(K,E(K,M)) = M$

Assumption

$D(–,\{M\}_K)$ is infeasible to compute when you don’t know K.

When is a cipher “secure”?

Perfect secrecy

- Knowing the ciphertext tells you nothing about the message.

- The probability of message M is the same as
the probability of message M given the ciphertext c.

- Implementation: Vernam Cipher (one-time pad).
All messages have same length.
Encrypt: XOR the key and the plaintext
Decrypt: XOR the key and the ciphertext
Important! Use the key only once!

Encryption

$E(K,M) = \{M\}_K = K \text{ xor } M$

Decryption

$D(K,\{M\}_K) = K \text{ xor } \{M\}_K$

Theorem

$$\begin{aligned}
D(K,E(K,M)) &= K \text{ xor } \{M\}_K \\
&= K \text{ xor } (K \text{ xor } M) \\
&= (K \text{ xor } K) \text{ xor } M \\
&= 0 \text{ xor } M \\
&= M
\end{aligned}$$

Perfect secrecy

- **Important! Use the key only once!**

- Vernon cipher not practical:
  Need as many bits of pre-agreed key as bits of plaintext.

- Think about how much mail you get.

- Need: fixed-size key for arbitrary amount of messages.

- Theorem (Shannon): Vernon cipher is optimal.
  Perfect secrecy requires as one bit key for each one bit of plaintext.

Block cipher

- Aka pseudo-random permutation

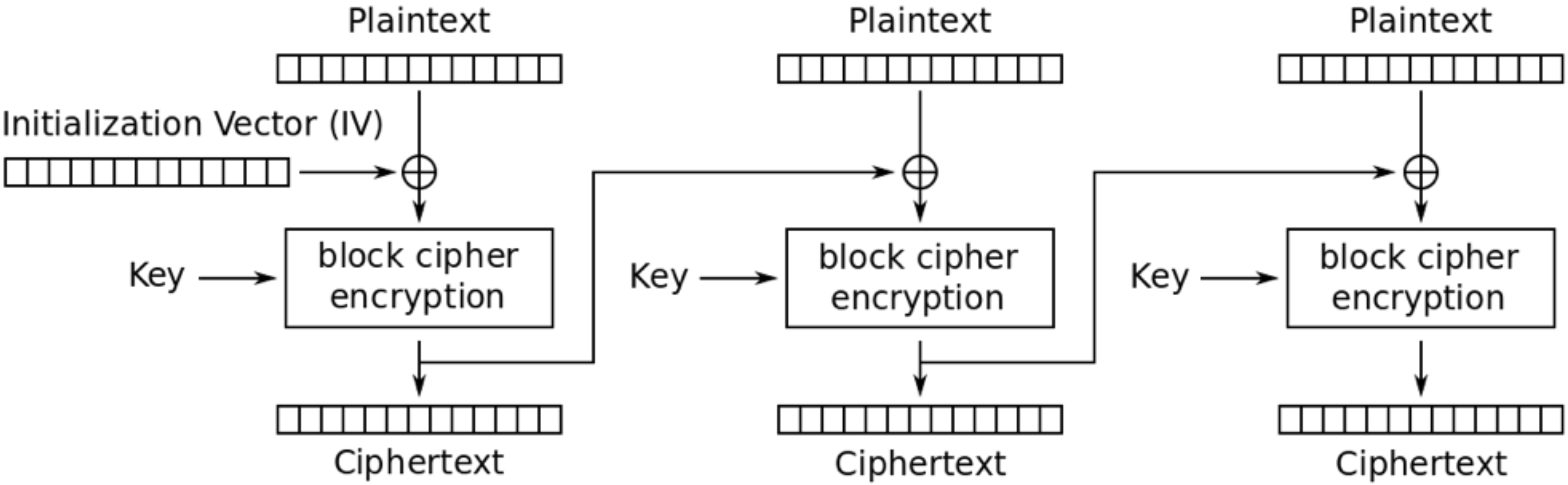
- Idea: Agree on short, fixed-length key.
  Generate a fixed-length permutation from this key.

- Problem: Frequency analysis.
  (Mono-alphabetic is an 8-bit permutation.)

- Solution: Add a random value on each use of the cipher, the *initialisation vector*.

- Multiple variants, we'll look at cipher-block chaining.

Cipher Block Chaining



NB! Nothing to do with blockchain/bitcoin.

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher_Block_Chaining_.28CBC.29

Definitions

π – permutation, needs key and block
K – secret key
M_i – i’th part of message
I – initialisation vector

Encryption

$B_0 = \pi(K, I \text{ xor } M_0)$
$B_i = \pi(K, B_{i-1} \text{ xor } M_0)$

Decryption

$D_0 = \pi(K, B_0) \text{ xor } I$
$D_i = \pi(K, B_i) \text{ xor } D_{i-1}$

Theorem

$$\begin{aligned} D_0 &= \pi(K, B_0) \text{ xor } I \\ &= \pi(K, \pi(K, I \text{ xor } M_0)) \text{ xor } I \\ &= (I \text{ xor } M_0) \text{ xor } I && (\pi(K,\pi(K,x)) = x) \\ &= M_0 \end{aligned}$$

Practice

- Shift cipher:
  rot13. Popular on usenet to mask movie spoilers.

- Perfectly secure ciphers:
  OTP/One-time pad/Vernam cipher.

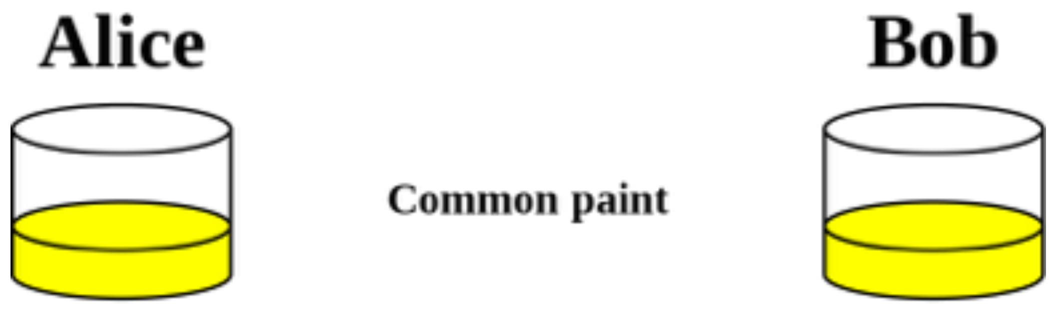
- Block ciphers:
  DES. Broken 1999, use **Triple-DES**.
  RC4. Weak. Prohibited in TLS. Multiple known attacks.
  AES (Rijndael). No known feasible attacks.

Symmetric scheme challenges

- Key distribution.
- E.g., how do a bank get key to every customer?
- In general, n parties need n^2 keys.

Asymmetric Encryption

Diffie-Hellman



- Establish a shared secret using only public messages

- Key idea: make a secret each, mix it with something public and they

https://commons.wikimedia.org/wiki/File:Diffie-Hellman_Key_Exchange.svg

Group theory in one slide

Definition
A *group* is a set with a multiplication operator.

Example
Natural numbers with multiplication. (Duh.)

If G is a group, g is an element of G, and n a number, we can write $g^n = g*g*…*g$.

Definition
A *cyclic group of order n* is a group where some element g generates the entire group:

$$G = \{g, g^2, g^3, …, g^n\}$$

Belief
Given g^a and g^b, computing g^{ab} is hard.

Diffie-Hellman in one slide

Agree on a cyclic group G of order n
Agree on a generator g of G

ALICE **BOB**

Pick secret a with $0 < a < n$
Send $A = g^a$ to Bob

Pick secret b with $0 < b < n$
Send $B = g^b$ to Alice

Compute $s = B^a$

Compute $s = A^b$

Theorem
Alice: $s = A^b = (g^a)^b = g^{ab}$
Bob: $s = B^a = (g^b)^a = g^{ba} = g^{ab}$

Security:
Given g^a and g^b, computing g^{ab} is hard.

Cyclic group and generator: Integers modulo.
Pick prime p and relative prime g. Order p-1
Say $p = 31$ and $g = 2$

ALICE **BOB**

Pick secret $a=7 < 31$
Send $A = g^a = 2^7 = 128$ to Bob

Pick secret $b=3 < 31$
Send $B = g^b = 2^3 = 8$ to Alice

Compute $s = B^a = 8^7 = 2097152$

Compute $s = A^b = 128^3 = 2097152$

Key insight:
Alice: $s = A^b = (2^7)^3 = 2^{21} = 2097152$
Bob: $s = B^a = (2^3)^7 = 2^{21} = 2097152$

Given 128 and 8, computing 2097152 is hard.

Assymmetric encryption schemes

- Every principal has a public and a private key.
- The private key is secret, only the principal knows it.
- The public key is, well, public, everyone may know it.
- Alice encrypts for Bob using *Bob's public key.*
- Bob decrypts with *Bob's private key*.

Definition, encryption:

$E(K_{pub}, M) = \{M\}_{Kpub}$

Decryption, decryption:

$D(K_{priv}, \{M\}_{Kpub}) = M$

Theorem:

$D(K_{priv}, E(K_{pub}, M)) = M$

Practice

- RSA
  (Algorithm, not company.
  RSA BSAFE likely compromised by NSA.)

- ElGamal

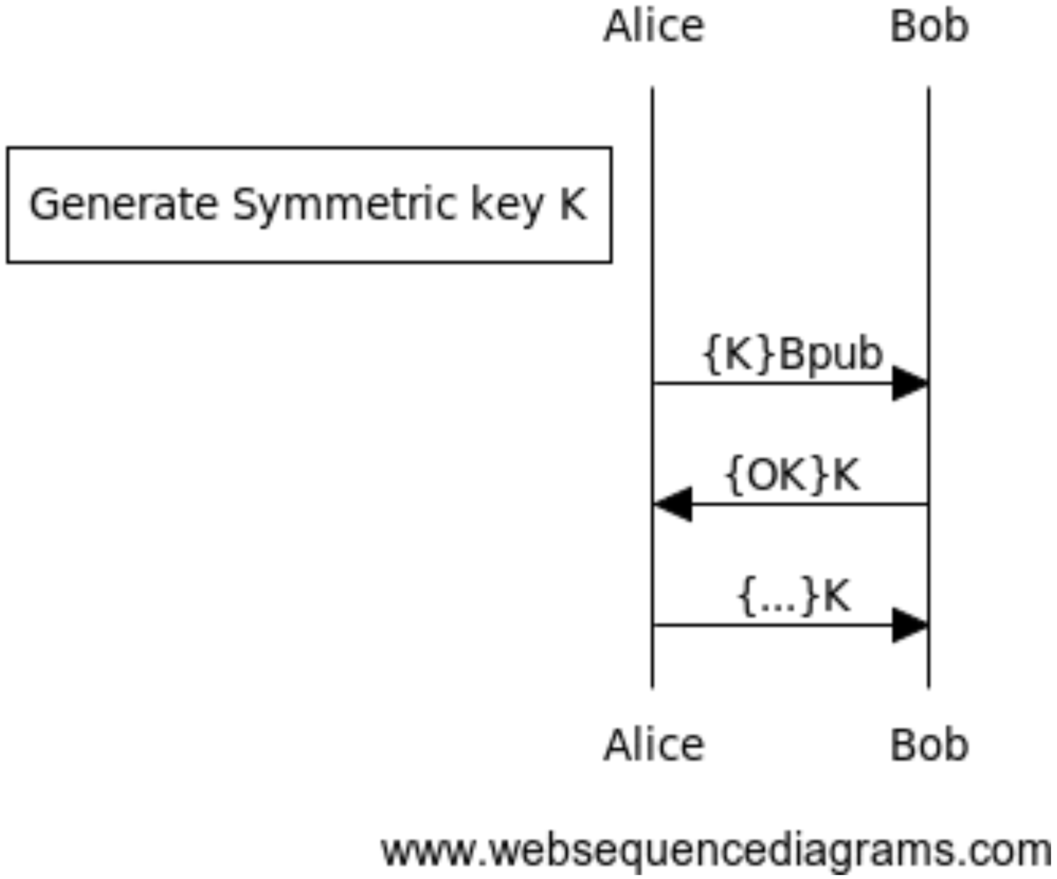
- Elliptic curves

Key distribution?

- Partially solves key distribution; now n parties need only n key-pairs.

Assymmetric Algorithms

- Slow to compute in practice
- Often used for agreeing on a secret key for a symmetric algorithm.
- RSA. Considered secure for sufficiently large key sizes. (768 bit key broken in 2009 using 2000 years of computing time.)

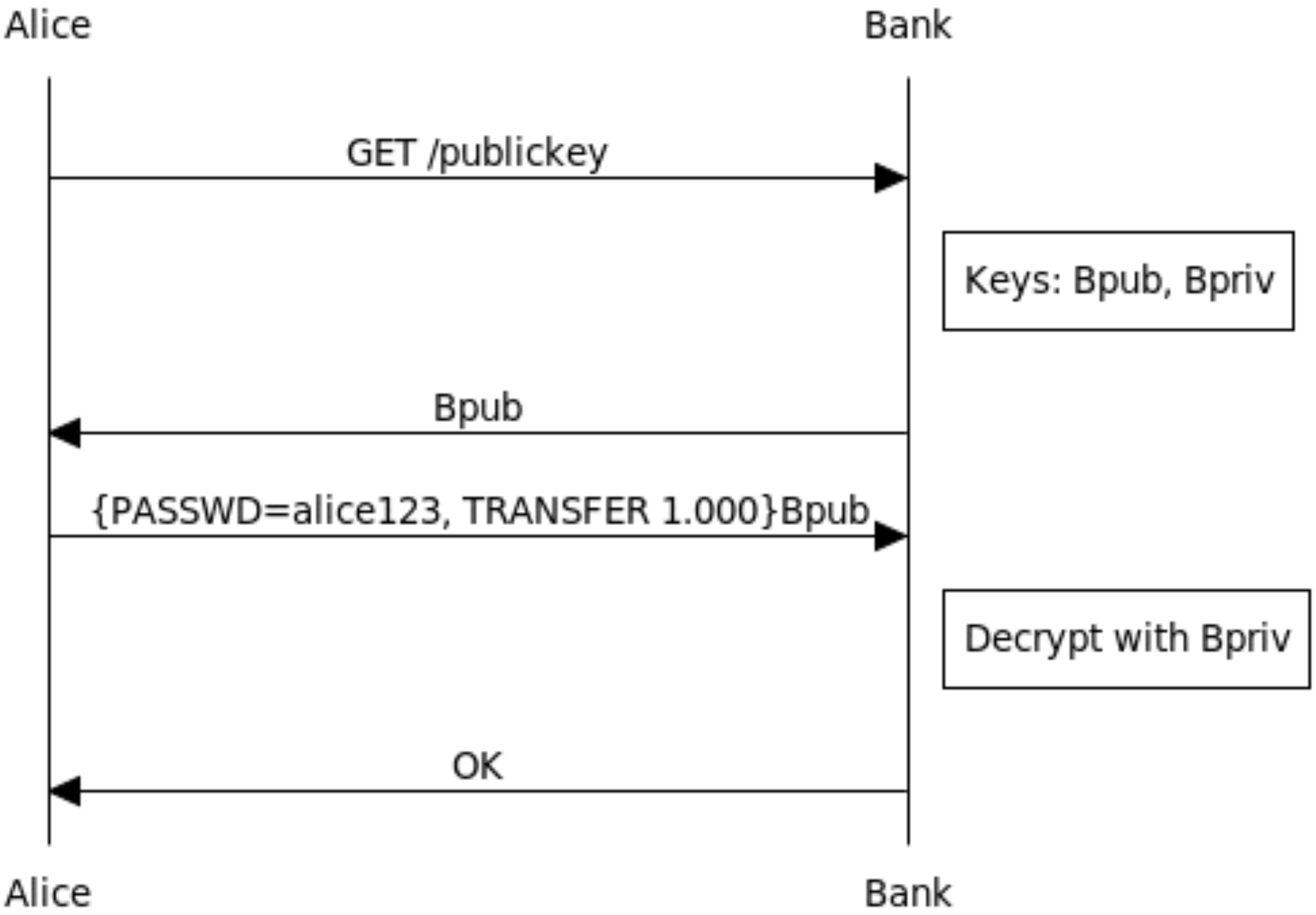


Question

- I'm a bank; my clients net secure net-banking.
- I put my public key K_{pub} on my webpage.
- Clients should:

  1. download the public key.
  2. encrypt their requests with my public key and send it to me.
  3. requests are now communicated securely.
- Yes? No?

That is, this?



Alice

Bank

GET /publickey

Keys: Bpub, Bpriv

Bpub

{PASSWD=alice123, TRANSFER 1.000}Bpub

Decrypt with Bpriv

OK

Alice

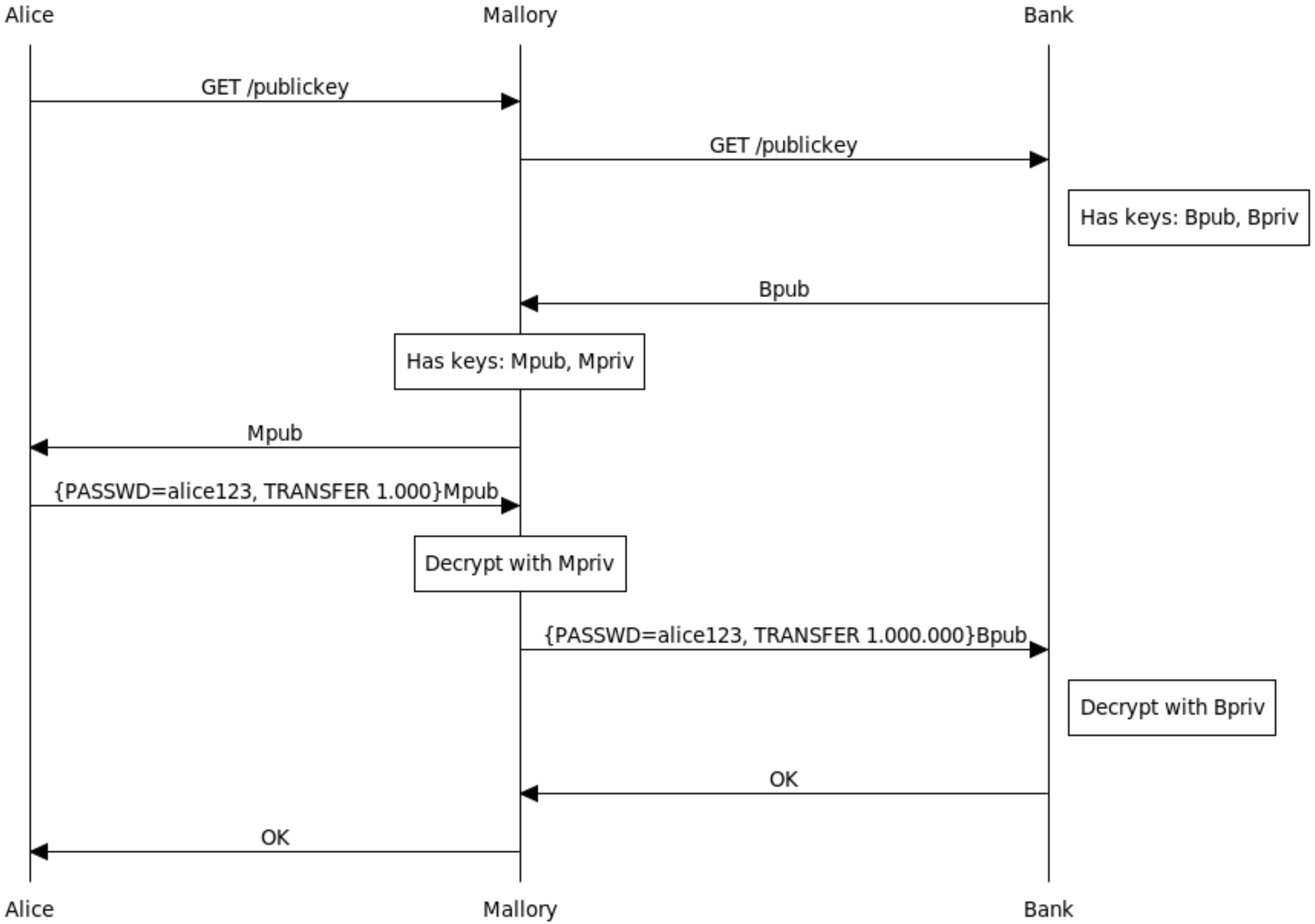
Bank

www.websequencediagrams.com

Man-in-the-middle attack

- No!

- If the adversary intercepts my traffice, he can replace the public key of the bank with his own.



Alice

Mallory

Bank

GET /publickey

GET /publickey

Has keys: Bpub, Bpriv

Bpub

Has keys: Mpub, Mpriv

Mpub

{PASSWD=alice123, TRANSFER 1.000}Mpub

Decrypt with Mpriv

{PASSWD=alice123, TRANSFER 1.000.000}Bpub

Decrypt with Bpriv

OK

OK

Alice

Mallory

Bank

www.websequencediagrams.com

What does this mean for Diffie-Hellman?

- (Exercise)

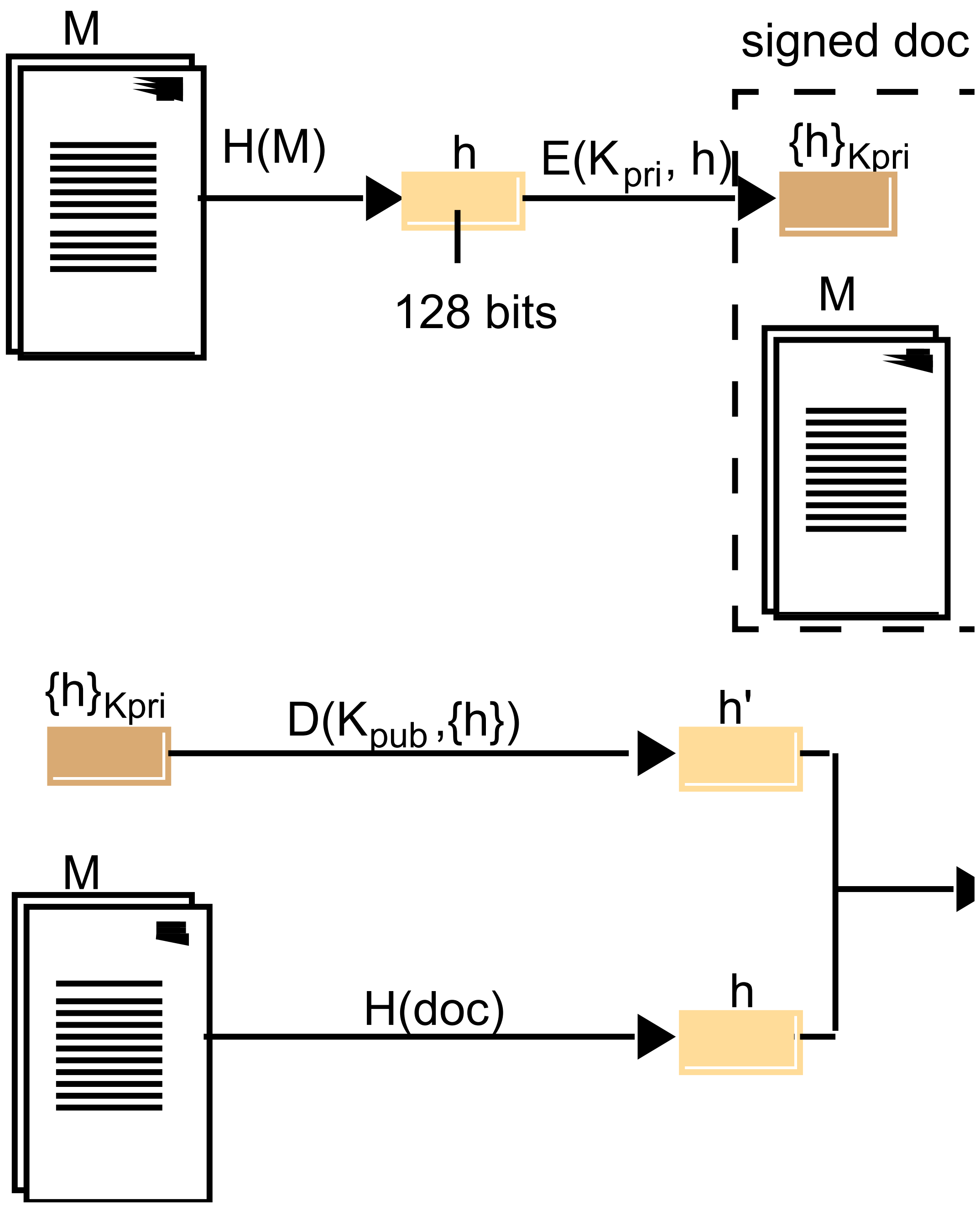
Signatures & Certificates

Signatures

- Authenticity of messages (signee, contents)
- Non-repudiability of messages

… with asymmetric scheme:

- I have keys K_{pub}, $K_{priv.}$ and a message M.
- I compute a digest (hash) H(M).
- I encrypt the hash with my *private* key S = E(K_{priv}, H(M))
- I send $[M]_K$ = M,S
- Recipient decrypts S with $K_{pub,}$ checks himself if H' = D($K_{pub,}$ S) =? H(M).
- Adversary can't tamper with M, because H' won't match H(M).



Certificates

- Signed public keys.

- I am a Certificate Authority. I have keys K_{pub}, $K_{priv.}$

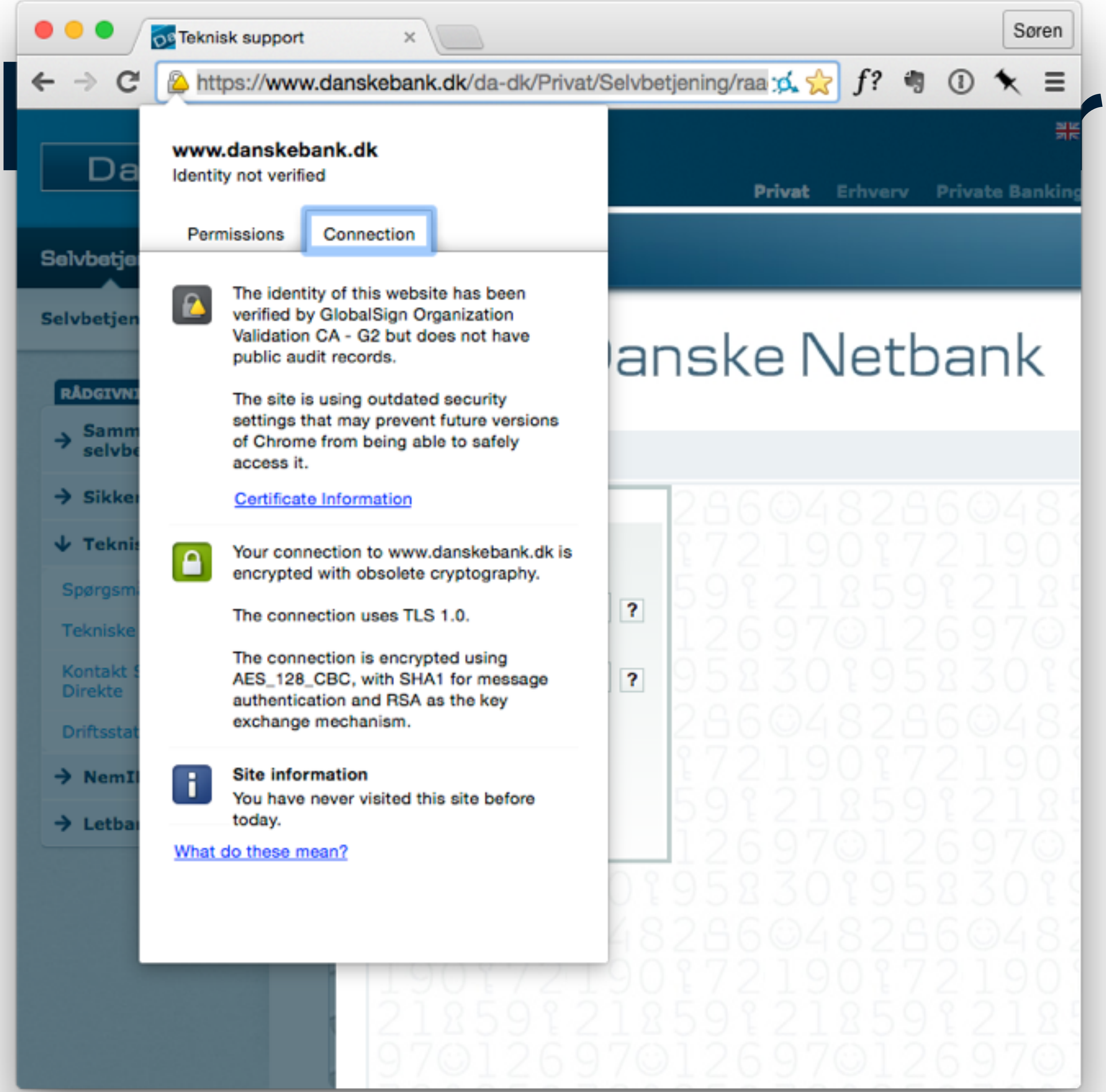
- The bank “International Bank A/S” has keys B_{pub}, B_{priv}.

- I sign a message M containing B_{pub} and the words “I believe this is the public key of International Bank A/S“, producing $S = E(K_{priv}, H(M))$. This is the certificate.

- Only I have Kpriv, so only I could have made such a certificate.

- International Bank A/S presents the certificate along K_{pub}.

- Anyone who has my public key can verify that I believe K_{pub} belongs to International Bank A/S.



www.danskebank.dk
Identity not verified

Permissions | Connection

The identity of this website has been verified by GlobalSign Organization Validation CA - G2 but does not have public audit records.

The site is using outdated security settings that may prevent future versions of Chrome from being able to safely access it.

Certificate Information

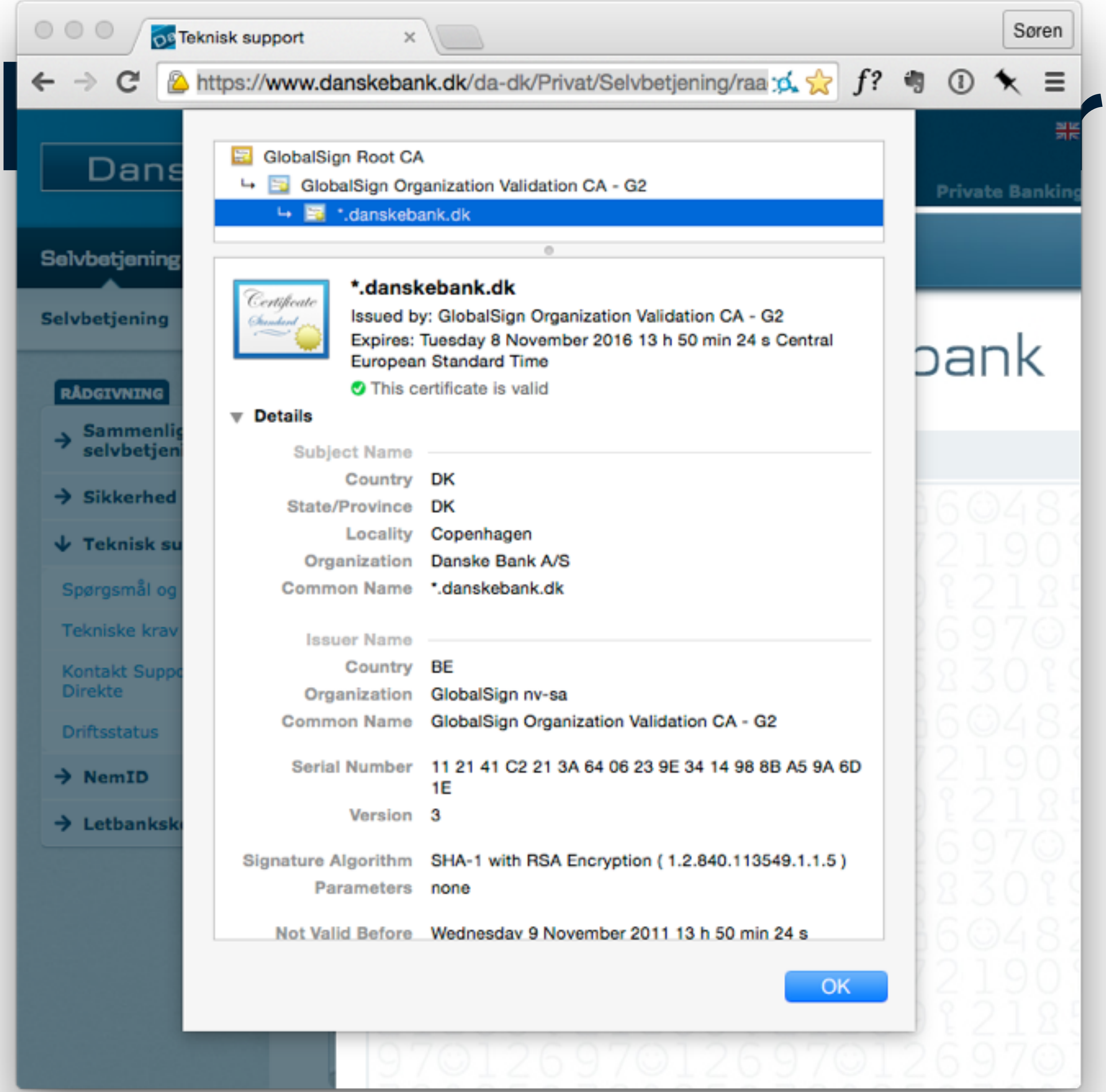
Your connection to www.danskebank.dk is encrypted with obsolete cryptography.

The connection uses TLS 1.0.

The connection is encrypted using AES_128_CBC, with SHA1 for message authentication and RSA as the key exchange mechanism.

Site information
You have never visited this site before today.

What do these mean?



GlobalSign Root CA
↳ GlobalSign Organization Validation CA - G2
↳ *.danskebank.dk

***.danskebank.dk**
Issued by: GlobalSign Organization Validation CA - G2
Expires: Tuesday 8 November 2016 13 h 50 min 24 s Central European Standard Time
✓ This certificate is valid

▼ **Details**

Subject Name	
Country	DK
State/Province	DK
Locality	Copenhagen
Organization	Danske Bank A/S
Common Name	*.danskebank.dk
Issuer Name	
Country	BE
Organization	GlobalSign nv-sa
Common Name	GlobalSign Organization Validation CA - G2
Serial Number	11 21 41 C2 21 3A 64 06 23 9E 34 14 98 8B A5 9A 6D 1E
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Wednesday 9 November 2011 13 h 50 min 24 s

TLS

- Transport Layer Security.

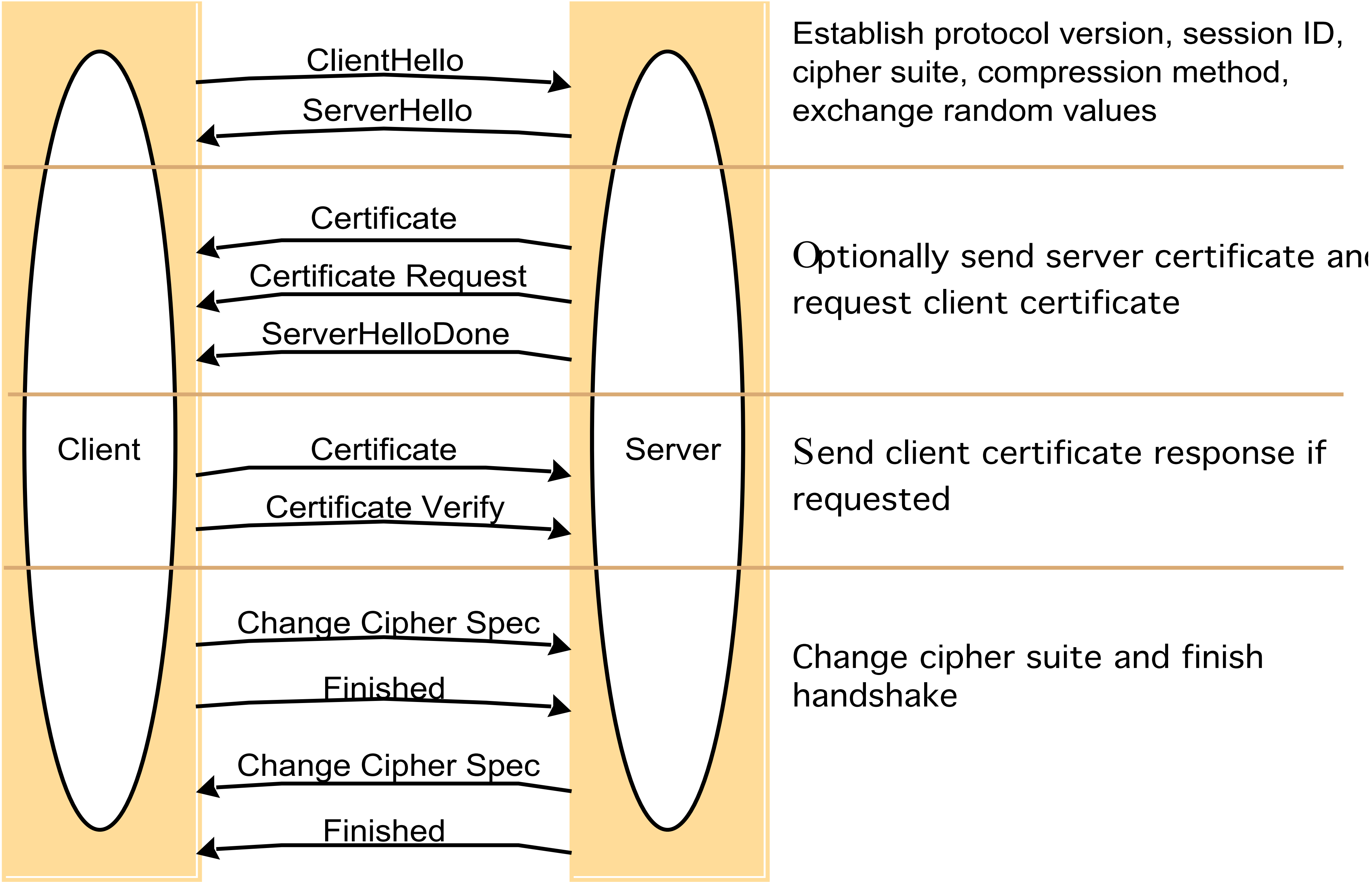
- Replaces earlier SSL. (viz. Danske Bank.)

- Handshake enables

exchange of certificates

agreement on symmetric key for subsequent encrypted communication.

TLS



Client

Server

ClientHello

ServerHello

Establish protocol version, session ID, cipher suite, compression method, exchange random values

Certificate

Certificate Request

ServerHelloDone

Optionally send server certificate an
request client certificate

Certificate

Certificate Verify

Send client certificate response if requested

Change Cipher Spec

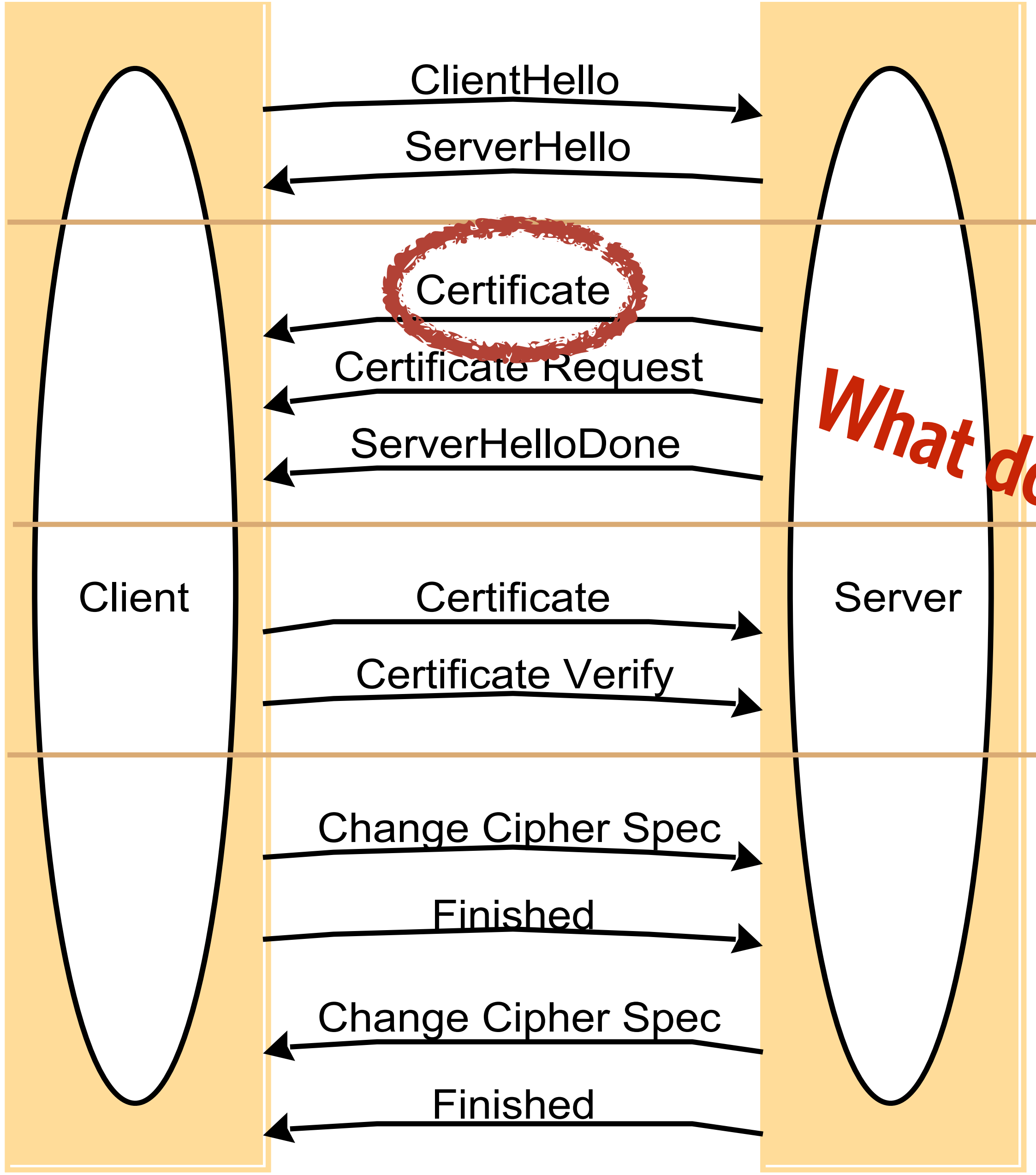
Finished

Change Cipher Spec

Finished

Change cipher suite and finish handshake

TLS



Client

Server

ClientHello

ServerHello

Establish protocol version, session ID, cipher suite, compression method, exchange random values

Certificate

Certificate Request

ServerHelloDone

Optionally send server certificate an request client certificate

What do I do with this?

Certificate

Certificate Verify

Send client certificate response if requested

Change Cipher Spec

Finished

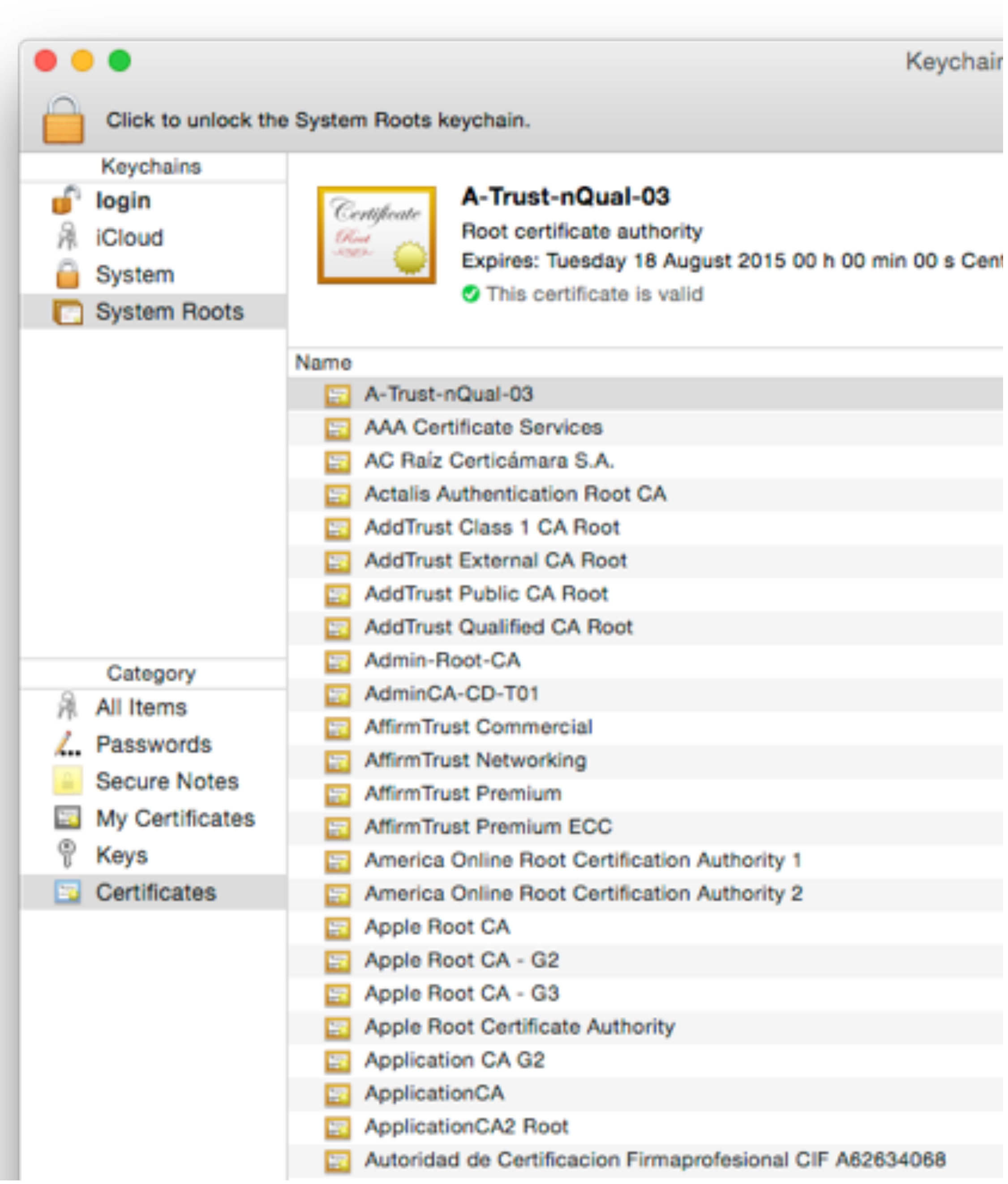
Change Cipher Spec

Finished

Change cipher suite and finish handshake

Certificates and the web

- X.509 certificates
- OSes, browsers come preloaded with “root” certificates from trusted Certificate Authorities.
- Root certificates are signed by themselves and thus implicitly trusted.
- (“Here is the public key of International Bank A/S; you can trust it because I have a certificate made with the corresponding private key” doesn’t give you any connection to International Bank A/S at all.)



Click to unlock the System Roots keychain.

A-Trust-nQual-03
Root certificate authority
Expires: Tuesday 18 August 2015 00 h 00 min 00 s Cen
✓ This certificate is valid

Name
A-Trust-nQual-03
AAA Certificate Services
AC Raíz Certicámara S.A.
Actalis Authentication Root CA
AddTrust Class 1 CA Root
AddTrust External CA Root
AddTrust Public CA Root
AddTrust Qualified CA Root
Admin-Root-CA
AdminCA-CD-T01
AffirmTrust Commercial
AffirmTrust Networking
AffirmTrust Premium
AffirmTrust Premium ECC
America Online Root Certification Authority 1
America Online Root Certification Authority 2
Apple Root CA
Apple Root CA - G2
Apple Root CA - G3
Apple Root Certificate Authority
Application CA G2
ApplicationCA
ApplicationCA2 Root
Autoridad de Certificacion Firmaprofesional CIF A62634068

Certificates and the web

- X.509 certificates
- OSes, browsers come preloaded with “root” certificates.
- Root certificates are signed by themselves and thus implicitly trusted.
- (“Here is the public key of International Bank A/S; you can trust it because I have a certificate made with the corresponding private key” doesn’t give you any connection to International Bank A/S at all.)
- A certificate you receive is signed by someone.
- Hopefully that someone is someone you trust.
- So you trust the browser.

SuperFish

- Lenovo shipped machines with a self-signed root certificate from a small company called SuperFish.

- SuperFish man-in-the-middled all HTTPS traffic on the local machine in order to insert ads.

- The root-certificate was insufficiently protected; anybody can certify anything for a SuperFish compromised machine.

- Check if your Lenovo machine is affected here (bottom): http://arstechnica.com/security/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections/

Summary

Summary

- Hashes
- Symmetric encryption schemes
- Asymmetric encryption schemes
- Signatures
- Certificates
- SSL/TLS

Questions?