

The Challenges of Web Security

James H. Davenport

University of Bath

12 November 2012

- ① How secure is the communication: can a third party eavesdrop on what is being shared?
- ② Is the “end” really who my device thinks it is, or am I the victim of a “man-in-the-middle” attack?
- ③ Is the “end” my device is talking to the entity I intend my device to be talking to?

The first two are essentially technical problems, but the third is definitely socio-technical.

We don't normally shout our PIN numbers out in crowded supermarkets, so why should we broadcast them on wireless networks?

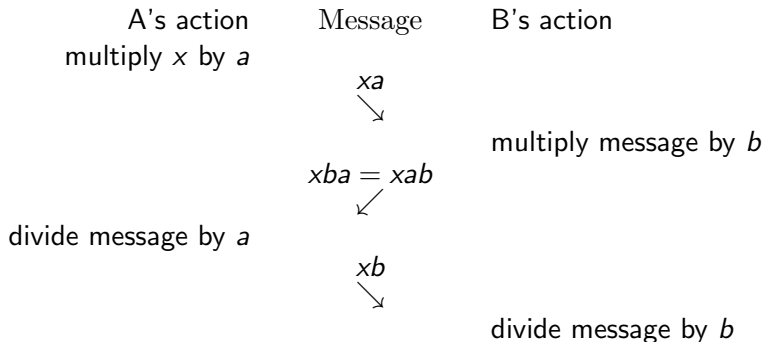
It's not only James Bond who wants cryptography?

Numbers rather than Padlocks (I)

Idea due to Diffie & Hellman (1976) [3]

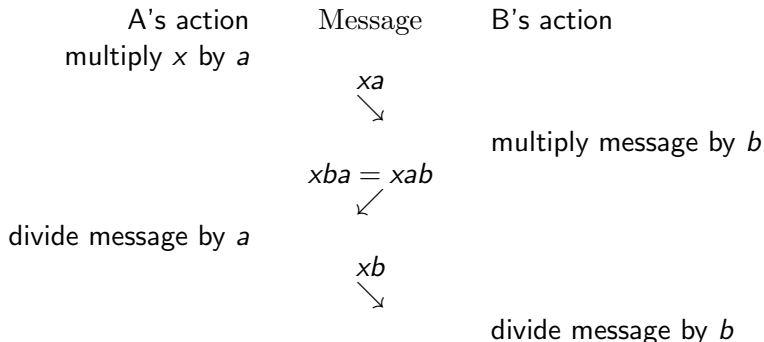
A wishes to send x to B.

A and B each think of a random number, say a and b .



In practice, to avoid guessing, and numerical errors, x , a and b are whole numbers modulo some *large* prime p .

Numbers rather than Padlocks (I) — snag

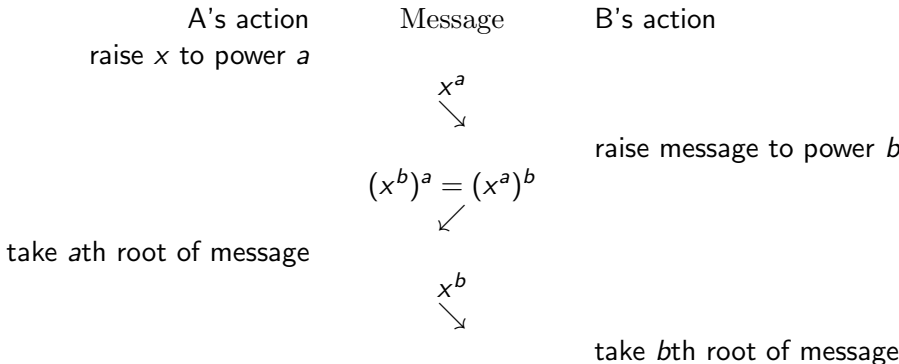


Eavesdropper computes $\frac{xa \cdot xb}{xab} = x$.

So replacing the padlocks by numbers has given the eavesdropper the chance of doing arithmetic.

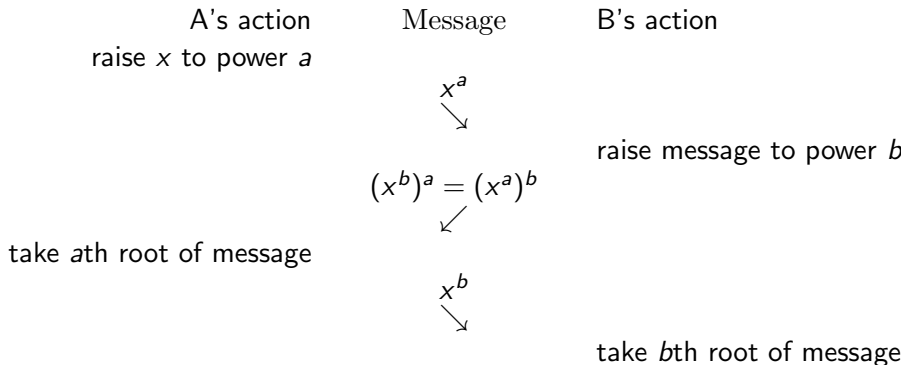
Numbers rather than Padlocks (II)

Let's be more subtle : upgrade from multiplication to powers.



Surely this frustrates the eavesdropper?

But what about logarithms?



Eavesdropper computes

$$\frac{\log(x^a) \cdot \log(x^b)}{\log(x^{ab})} = \frac{a \log(x) \cdot b \log(x)}{ab \log(x)} = \log(x).$$

Essentially the same trick as before, but with logarithms!

Do logarithms exist?

Remember that we are working modulo a *large* prime p . For simplicity, I will take $p = 41$, since it's small enough, and logs base 7, so that $\log(7) = 1$.

1	2	3	4	5	6	7	8	9	10
0						1			
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

So $\log(49) = 2$, but $49 = 1 \cdot 41 + 8 \equiv 8$ since we are working modulo 41, and $\log(7 \cdot 8) = 3$, but $7 \cdot 8 = 56 \equiv 15$, so $\log(15) = 3$.

Do logarithms exist?

Remember that we are working modulo a *large* prime p . For simplicity, I will take $p = 41$, since it's small enough, and logs base 7, so that $\log(7) = 1$.

1	2	3	4	5	6	7	8	9	10
0						1	2		
11	12	13	14	15	16	17	18	19	20
				3					
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40

And we can fill in: $8 \cdot 8 = 64 \equiv 23$, so $\log(23) = 4$. Also $8 \cdot 15 = 120 \equiv -3 = 38$ so $\log(38) = 2 + 3 = 5$ and $\log(9) = 10$.

Do logarithms exist?

Remember that we are working modulo a *large* prime p . For simplicity, I will take $p = 41$, since it's small enough, and logs base 7, so that $\log(7) = 1$.

1	2	3	4	5	6	7	8	9	10
0						1	2	10	
11	12	13	14	15	16	17	18	19	20
				3					
21	22	23	24	25	26	27	28	29	30
		4							
31	32	33	34	35	36	37	38	39	40
							5		

$15^2 \equiv 20$, so $\log(20) = 6$. $20^2 = 400 \equiv 31$, so $\log(31) = 12$.

Do logarithms exist?

Remember that we are working modulo a *large* prime p . For simplicity, I will take $p = 41$, since it's small enough, and logs base 7, so that $\log(7) = 1$.

1	2	3	4	5	6	7	8	9	10
0						1	2	10	
11	12	13	14	15	16	17	18	19	20
				3					6
21	22	23	24	25	26	27	28	29	30
		4							
31	32	33	34	35	36	37	38	39	40
12							5		

and we can keep going, but it's a tedious process:

p operations for a table

methods taking roughly \sqrt{p} operations are known, and faster

methods taking roughly $e^{c\sqrt{\log p \log \log p}}$ operations, or even

$e^{c' \sqrt[3]{\log p \log^2 \log p}}$ operations, but it's still tedious!

Simplicity can be dangerous

- Not all p are equally difficult!
- In particular, we would like p to be such that $q = \frac{p-1}{2}$ is also prime, so that q is a *Sophie Germain* prime
- **Conjecturally**, there are infinitely many of these



Also, beware of shortcuts! In the 1980s, the Federal Reserve Bank needed such a system, and used $GF(2^{127})$ rather than a prime near that.

- Coppersmith [1] broke this with a $e^{1.35 \sqrt[3]{\log p \log^2 \log p}}$ attack, pragmatically 7 hours CPU on a 38.5MHz machine (one of the fastest in the world in 1982!).

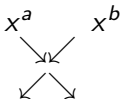
But it takes three messages

sequentially. Can we do better? Let x be a **public** number. Again, A and B choose random numbers a and b .

A's action
raise x to power a

Message

B's action
raise x to power b



raise message to power a
 $(x^b)^a$

raise message to power b
 $(x^a)^b$

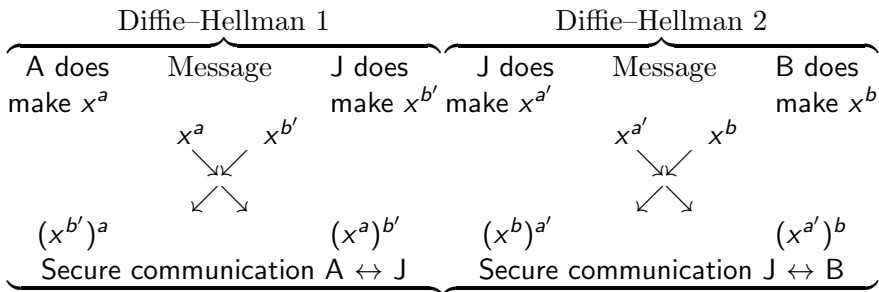
Now they are *both* in possession of $(x^a)^b = (x^b)^a$, which can be used as the key for any standard cipher.

Two messages, and in parallel!

This is *one* reason why secure websites display a padlock: to assure you that they have gone through this process between *your* browser and the web site: so the *communication* is secure.

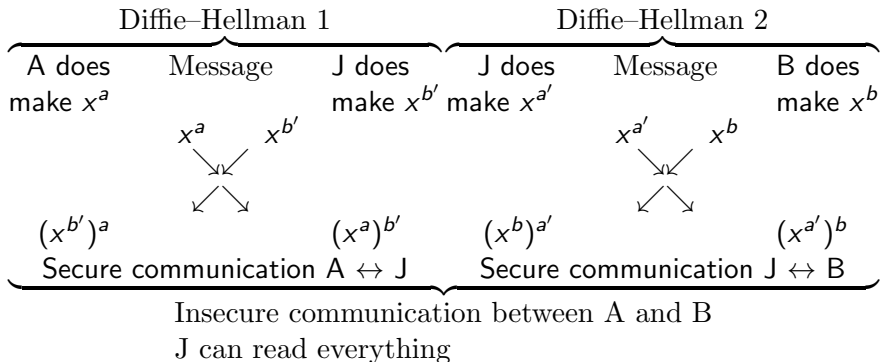
The man in the middle (also known as Janus)

Again, A and B choose random numbers a and b .
But J chooses a' and b' .



The man in the middle (also known as Janus)

Again, A and B choose random numbers a and b .
But J chooses a' and b' .



Public Secrets! (I)

Original idea due to Rivest, Shamir & Adleman (1977) [6]

The analogy is with a signature: anyone who knows my signature can check that it's mine, but in principle only I can produce it

Theorem (Fermat's Little Theorem (special case))

Let $N = pq$ where p, q are different primes, then

$$m^{N-p-q+1} \equiv 1 \pmod{N}$$

(provided m is not divisible by p or q)

Corollary (RSA)

If $de \equiv 1 \pmod{N - p - q + 1}$, $(m^e)^d \equiv m \pmod{N}$

We think of e as the **encryption** exponent, and d as the **decryption** exponent

Therefore, if I

- publish (my) N and d , but keep e (and p, q) secret
- Send you $c := m^e \pmod{N}$.
- You can compute $c^d = (m^e)^d \equiv m \pmod{N}$
- and be sure that only I could have constructed c

Of course m must be self-identifying

Breaking Public Secrets!

- Clearly *if* I can factor N , compute p and q , then I can compute e
- Factoring is hard! Best known algorithms again take $e^{c\sqrt[3]{\log N \log^2 \log N}}$, with $c \approx 7.1$.
- The current world record is a 768-bit number [4], using 2000 CPU-years (and 2 elapsed years)
- A 1024-bit number would be 10^{11} times as difficult
- *If* I know d , e , then I can factor N [2]



Nothing precludes there being a way of computing c some other way

The Real Problem is Publishing

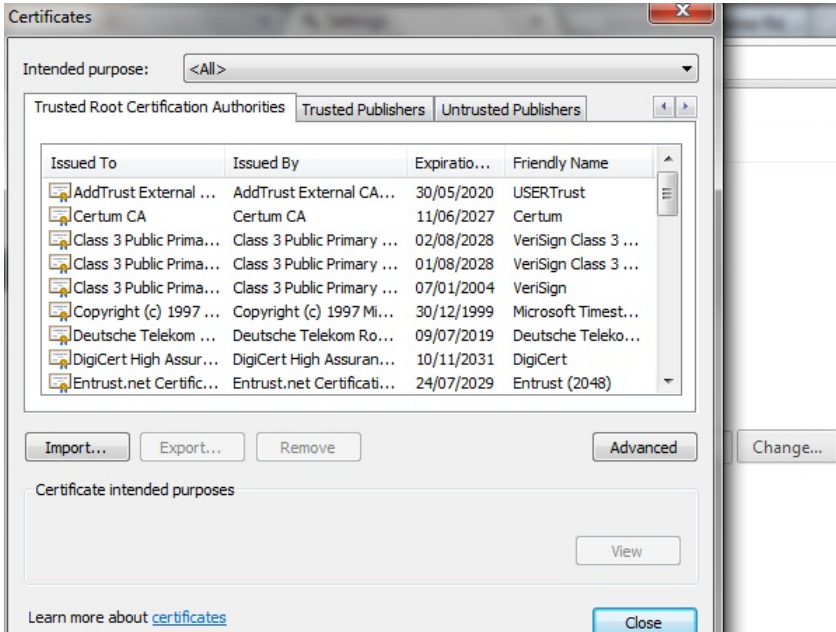
Original idea was literally that: XX Bank would publish the number in the paper

- Certificates are quite long 2×1024 bits = 512 hexadecimal digits (compared with 8 or 16 for a wireless key)
- My bank, and my supermarket, and my railway company, and Amazon, and ...
- How do I guarantee genuineness?

Hence what we need is a **Public Key Infrastructure** (PKI)

- Your browser has certain “Certificate Authorities” built into it
-
-
-

today's Web Public Key Infrastructure (Chrome)



The screenshot shows the Windows Certificates dialog box with the 'Trusted Root Certification Authorities' tab selected. The 'Intended purpose' dropdown is set to '<All>'. Below the tabs, a table lists various certification authorities. At the bottom, there are buttons for 'Import...', 'Export...', 'Remove', 'Advanced', and 'Change...'. A 'Certificate intended purposes' section is also visible with a 'View' button. At the very bottom, there is a link to 'Learn more about certificates' and a 'Close' button.

Intended purpose: <All>

Trusted Root Certification Authorities | Trusted Publishers | Untrusted Publishers

Issued To	Issued By	Expiratio...	Friendly Name
AddTrust External ...	AddTrust External CA...	30/05/2020	USERTrust
Certum CA	Certum CA	11/06/2027	Certum
Class 3 Public Prima...	Class 3 Public Primary ...	02/08/2028	VeriSign Class 3 ...
Class 3 Public Prima...	Class 3 Public Primary ...	01/08/2028	VeriSign Class 3 ...
Class 3 Public Prima...	Class 3 Public Primary ...	07/01/2004	VeriSign
Copyright (c) 1997 ...	Copyright (c) 1997 Mi...	30/12/1999	Microsoft Timest...
Deutsche Telekom ...	Deutsche Telekom Ro...	09/07/2019	Deutsche Telekom...
DigiCert High Assur...	DigiCert High Assuran...	10/11/2031	DigiCert
Entrust.net Certific...	Entrust.net Certificati...	24/07/2029	Entrust (2048)

Import... Export... Remove Advanced Change...

Certificate intended purposes View

Learn more about [certificates](#) Close

- Your browser has certain “Certificate Authorities” built into it
- And these are used to sign the certificates of sites
-
-

today's Web Public Key Infrastructure (Firefox)

The screenshot shows the Firefox Page Info dialog box for the URL <https://myweps.com/moodle23/login/index.php>. The Security tab is selected, displaying the following information:

Website Identity

- Website: **myweps.com**
- Owner: **This website does not supply ownership information.**
- Verified by: **Network Solutions L.L.C.**

[View Certificate](#)

Privacy & History

Have I visited this website prior to today?	Yes, 33 times	
Is this website storing information (cookies) on my computer?	Yes	View Cookies
Have I saved any passwords for this website?	Yes	View Saved Passwords

Technical Details

Connection Encrypted: High-grade Encryption (Camellia-256, 256 bit keys)
The page you are viewing was encrypted before being transmitted over the Internet.

- Your browser has certain “Certificate Authorities” built into it
- And these are used to sign the certificates of sites
- Quite possibly through several layers
-

today's Web Public Key Infrastructure (Firefox)

php

Information.

[View Certificate](#)

Yes, 33 times

Yes [View Cookies](#)

Yes [View Saved Passwords](#)

256-bit keys

transmitted over the Internet.

able to view information traveling between
this page as it traveled across the network.

Thunderbir... Thunderbir... Bonn10.pdf ... 343.pdf (ap... WEPS

Certificate Viewer: "myweeps.com"

General Details

Certificate Hierarchy

- AddTrust External CA Root
 - Network Solutions DV Server CA
 - myweeps.com

Certificate Fields

- Certificate Key Usage
- Certificate Basic Constraints
- Extended Key Usage
- Certificate Policies
- CRL Distribution Points
- Authority Information Access
- Certificate Subject Alt Name
- Certificate Signature Algorithm**
- Certificate Signature Value

Field Value


PKCS #1 SHA-1 With RSA Encryption

- Your browser has certain “Certificate Authorities” built into it
- And these are used to sign the certificates of sites
- Quite possibly through several layers
- If this doesn't check out, you get a warning

today's Web Public Key Infrastructure (Chrome)

SSL Error

← → ↻ 🏠 <https://moodle-test.bath.ac.uk/login/index.php>

 **This is probably not the site you are looking for!**

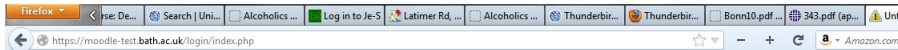
You attempted to reach **moodle-test.bath.ac.uk**, but instead you actually reached a server identifying itself as **moodle.bath.ac.uk**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **moodle-test.bath.ac.uk**.

You should not proceed, **especially** if you have never seen this warning before for this site.

▶ [Help me understand](#)

Windows taskbar icons: Start, File Explorer, Chrome, Firefox, Word, Skype, PDF Reader, Paint, Calendar (16), OneDrive, Mail, Photos, System tray.

today's Web Public Key Infrastructure (Firefox 1)



This Connection is Untrusted

You have asked Firefox to connect securely to **moodle-test.bath.ac.uk**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

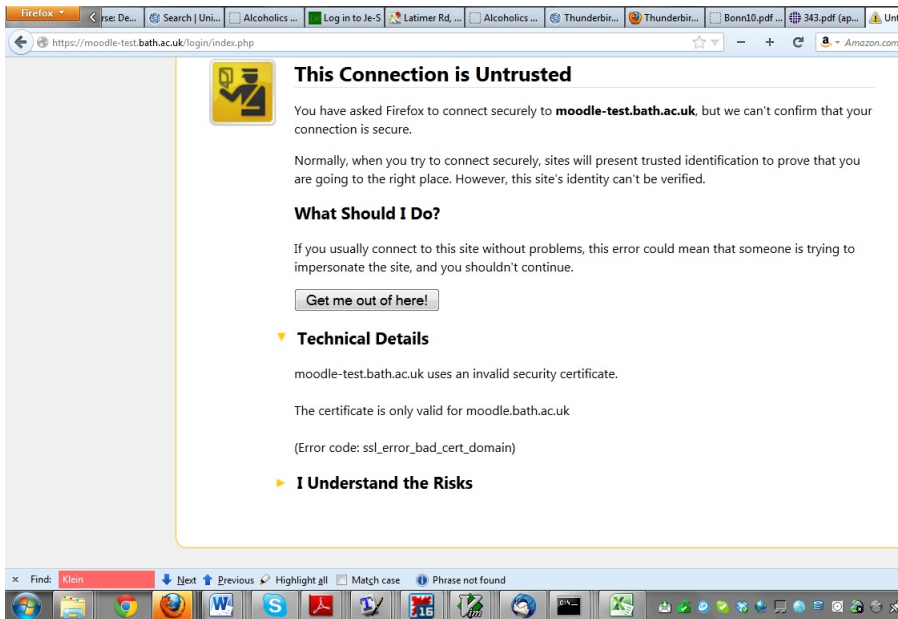
[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

Find: Klein Next Previous Highlight all Match case Phrase not found



today's Web Public Key Infrastructure (Firefox 2)



The screenshot shows a Firefox browser window with the address bar displaying `https://moodle-test.bath.ac.uk/login/index.php`. The main content area features a yellow warning icon of a person with a question mark, followed by the heading **This Connection is Untrusted**. Below the heading, the text reads: "You have asked Firefox to connect securely to **moodle-test.bath.ac.uk**, but we can't confirm that your connection is secure." It further explains that normally sites present trusted identification, but in this case, the site's identity cannot be verified. A section titled **What Should I Do?** suggests that if the user usually connects without problems, this error could mean someone is impersonating the site, and they should not continue. A button labeled **Get me out of here!** is provided. A **Technical Details** section states that `moodle-test.bath.ac.uk` uses an invalid security certificate, which is only valid for `moodle.bath.ac.uk`, with an error code of `ssl_error_bad_cert_domain`. A final section, **I Understand the Risks**, is partially visible. The browser's search bar at the bottom shows the word "Klein" and various search options like "Next", "Previous", "Highlight all", "Match case", and "Phrase not found". The Windows taskbar at the very bottom shows several application icons, including Internet Explorer, Firefox, Word, Skype, and various system tray icons.

Firefox ▾ | < | rse: De... | Search | Uni... | Alcoholics ... | Log in to Je-S | Latimer Rd, ... | Alcoholics ... | Thunderbir... | Thunderbir... | Bonn10.pdf ... | 343.pdf (ap... | Un

← | <https://moodle-test.bath.ac.uk/login/index.php> | ☆ | - | + | ↻ | a - Amazon.com

This Connection is Untrusted

You have asked Firefox to connect securely to **moodle-test.bath.ac.uk**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

▼ Technical Details

moodle-test.bath.ac.uk uses an invalid security certificate.

The certificate is only valid for moodle.bath.ac.uk

(Error code: ssl_error_bad_cert_domain)

▶ I Understand the Risks

Find: Klein | Next | Previous | Highlight all | Match case | Phrase not found

Windows taskbar: Internet Explorer, Firefox, Word, Skype, PDF, 16, 3m, Mail, Photos, System tray icons.

This System has its Flaws

- There's no mechanism for revoking a certificate:
- we just have to wait for it to expire
- (and certainly not of a root certificate, where the expiry periods are **long**)
- My biggest worry is about some of the intermediate authorities



There are various technical chinks in the armour

- Especially for cloud-based servers [5]

Nevertheless it seems to work pretty well from a technical point of view

Human Beings have their Flaws

- Getting a certificate is pretty easy



1



¹Pointed out by the audience

The Human Side of Security (Thawte)

Firefox | < | Use: De... | Search | Uni... | Alcoholics ... | Log in to Je-S | Latimer Rd, ... | Alcoholics ... | Thunderbir... | Thunderbir... | Thawte ... x | 343.pdf (ap... | WE

Thawte, Inc. (US) | https://ssl-certificate-center.thawte.com/process/retail/product_selector?sessionId=B874B5343D4893FD801A2FB88C35E7D?uid=fe7 | - + C | Amazon.com



[Help & Support](#) | [Feedback](#)

Buy ▶ 1) Options ▶ 2) Technical Contact ▶ 3) CSR ▶ 4) Contacts ▶ 5) Sign In ▶ 6) Payment ▶ 7) Summary

CHAT WITH US
A Representative is Standing By.

Select a level of security

<input type="radio"/> SSL Web Server Certificate with EV Standard Encryption Highest Trust		<ul style="list-style-type: none">Green address barExtended Validation40-bit minimum to 256-bit SSL encryption Learn more...
<input type="radio"/> SGC SuperCert Strongest Encryption Established Trust		<ul style="list-style-type: none">Full organization validation128-bit minimum to 256-bit SSL encryption Learn more...
<input type="radio"/> SSL Web Server Certificate Standard Encryption Established Trust		<ul style="list-style-type: none">Full organization validation40-bit minimum to 256-bit SSL encryption Learn more...
<input checked="" type="radio"/> SSL 123 Certificate Standard Encryption Issued in 1 business day, or less		<ul style="list-style-type: none">Domain validation40-bit minimum to 256-bit SSL encryption Learn more...

Total: US \$149

SSL123 Certificate
Validity period: 1 year
Number of server licenses: 1
Number of Subject Alternative Names: 0

Do you already have a Certificate Center sign-in?

* Username

* Password

[Sign in](#)

[Forgot your username?](#)

[Forgot your password?](#)

If you do not have a Certificate Center account, click "Continue" at the bottom of the page to proceed and create an account later.

Select validity period

1 year

Find: Klein | Next | Previous | Highlight all | Match case | Phrase not found



The Human Side of Security (Thawte)

Firefox | < | Use: De... | Search | Uni... | Alcoholics ... | Log in to Je-S | Latimer Rd, ... | Alcoholics ... | Thunderbir... | Thunderbir... | Thawte ... x | Thawte - Kn... | 343

Thawte, Inc. (US) | https://ssl-certificate-center.thawte.com/process/retail/capture_tech_contact_details.do

Buy > 1) Options > 2) Technical Contact > 3) CSR > 4) Contacts > 5) Sign In > 6) Payment > 7) Summary

CHAT WITH US

A Representative is Standing By.

Technical contact: State/Province is required.

Enter technical contact ?

* Required fields

* Email:

* First name:

* Last name:

* Job title:

* Telephone:

Fac:

* Company name:

* Address 1:

Address 2:

* City:

* State/Province:

* ZIP/Postal code:

* Country:

Total: US \$149

SSL123 Certificate
Validity period: 1 year
Number of server licenses: 1
Number of Subject Alternative Names: 0

Total: US \$149

< Back

Cancel

Continue

Legal Notices | Privacy | Repository | © 2012 Thawte, Inc. All rights reserved.

Find: Klein | Next | Previous | Highlight all | Match case | Phrase not found

Windows taskbar icons: Internet Explorer, Firefox, Chrome, Word, Skype, PDF Reader, Paint, etc.

Human Beings have their Flaws

- Getting a certificate is pretty easy
- Basically, all you need is to be `postmaster@mydomain.co.uk` to get the certificate e-mailed to you
- And getting the domain is easy
- 5 minutes and £5.39 to get `JamesDavenport.me.uk`
- And probably `www.british-airway.co.uk`
- Or many other forms of “typo-squatting” (such as expiry-date squatting)²

²Pointed out by the audience

Solutions?

Whoever thinks his problem can be solved using cryptography, doesn't understand his problem and doesn't understand cryptography.

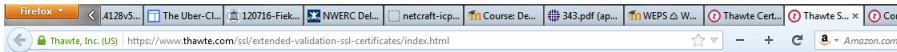
Attributed by Roger Needham and Butler Lampson to each other

Basically, two families of solutions

- Certificate-based solutions, such as “Extended Verification”



Extended validation (Thawte)



Contact Us: 1-888-484-2983

Chat sales@thawte.com

Change Coun



Products

Partners

Support

Resources

My Account

SEARCH



products

SSL Certificates
[Compare All]

• **SSL Web Server
Certificates with
EV**

• SSL Web Server
Certificates

• SGC SuperCerts

• SSL 123
Certificates

• SAN/UC Capable
Certificates

• Wildcard SSL
Certificates

• Volume SSL
Discounts

Code Signing
Certificates

Thawte Trusted Site
Seal

US Home > Products > SSL Certificates > SSL Web Server Certificates with EV



Email



Share



Print

ssl web server certificates with ev

ESTABLISHES TRUST AND SECURITY AT A GLANCE

Thawte® SSL Web Server Certificates with EV enable the most visible security indicator: the green address bar in high-security browsers, assuring users that your site is secure and your identity has been authenticated to the industry's highest standard. When customers see the green address bar and the Thawte® Trusted Site Seal, they gain the confidence to complete their transaction. SSL Web Server Certificates with EV include Extended Validation, the [Thawte Trusted Site Seal](#), free issuances, and a 30-day money back guarantee.

<https://www.woodgrovebank.com>

Thawte Inc [US]

*Internet Explorer 7+

Note: Thawte SSL Web Server Certificate with EV is a chained SSL certificate and your web server must support certificate chaining. [Learn more](#)

1 year - \$599

BUY

RENEW

Benefits and Features

Volume Discounts

Choosing a Certificate

Support

- **Increase revenue potential and reduce fraud** with the green address bar and the Thawte Trusted Site Seal, which is available in 18 languages.
- **Protect confidential information** exchanged during shopping, banking, secure sign in, and account self-service interactions with up to 256-bit SSL encryption and a 750k USD warranty.

contact sales

US toll-free: +1 888 484

South Africa:

+27 21 819 2800

Germany:

+49 69 3807 89081

France: +33 1 57 32 42

UK: +44 203 450 5486

[Submit Inquiry Online](#)

live help

SELECT A CHAT

New! Thawte

SAN Certificate

Now fully compatible
for Microsoft Unified
Communications
(UC) applications.



[LEARN MORE](#)



Solutions?

Whoever thinks his problem can be solved using cryptography, doesn't understand his problem and doesn't understand cryptography.

Attributed by Roger Needham and Butler Lampson to each other

Basically, two families of solutions

- Certificate-based solutions, such as “Extended Verification”



How much “extended validation” can the CA purchase for the price difference: \$450?

- Name-based solutions, such as Nominet's .uk proposal

Nominet's .uk proposal

http://www.nominet.org.uk/sites/default/files/Nominet_FINAL_electronic_form3_0.pdf

To further support the economic growth of the UK internet, we are holding a three month consultation about the potential introduction of a new service known as direct.uk, which would be specifically designed for businesses that are or want to get online, with a new shorter domain name of internet.uk rather than internet.co.uk.

Proposed key features include; verification to check a registrant has a UK address, daily monitoring for malicious software and viruses, and a digital signature which minimises the risks of a domain name being hijacked. These measures would be supported by a trustmark to give consumers a clear sign that it was a verified domain name.

References



D. Coppersmith.

Fast Evaluation of Logarithms in Fields of Characteristic Two.
IEEE Trans. Information Theory, IT-30:587–594, 1984.



J.-S. Coron and A. May.

Deterministic Polynomial-Time Equivalence of Computing the RSA Secret Key and Factoring.

J. Cryptology, 20:39–50, 2007.



W. Diffie and M.E. Hellman.

New Directions in Cryptography.

IEEE Trans. Inform. Theory, IT-22:644–654, 1976.



T. Kleinjung, K. Aoki, J. Franke, A.K. Lenstra, E Thomé, J.W. Bos, P. Gaudry, A. Kruppa, P.L.

Montgomery, D.A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann.

Factorization of a 768-bit RSA modulus.

In T. Rabin, editor, *Proceedings CRYPTO 2010*, pages 333–350.



T. Ristenpart and S. Yilek.

When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography.

In *Proceedings ISOC NDSS 2010*, 2010.



R.L. Rivest, A. Shamir, and L. Adleman.

U.S. Patent 4405829 — Cryptographic Communications System and Method.