Bill Clinton, Bertie Ahern[1], and digital signatures
(a **MAPLE** based introduction to public-key cryptography)

John Cosgrave, Mathematics Department,
St Patrick's College, Drumcondra,
Dublin 9, IRELAND
John.Cosgrave@spd.dcu.ie

Introduction. My ICTCM16 talk–with the above title–was delivered using **MAPLE**, and is available in active **mws**[2] and **html**[3] text formats in the *Public and other lectures* section of my web site (**[1]**). A hard copy of the former runs to over twenty-two A4 printed pages, and this shorter paper may be read as an extended introduction.

Background to the title of my ICTCM16 talk. Since1995-96 I have taught a third year undergraduate course *Number Theory and Cryptography* (using **MAPLE**) every year at St Patrick's College. Before I had a web site, David Joyner[4] at the United States Naval Academy (Annapolis) asked if I would allow that my course **MAPLE** worksheets be displayed at his site; they are still there at (**[2]**). Since June 1999 I have had my own web site, and there I have made available all course materials[5]: Word notes, **MAPLE** worksheets, and examination papers (3-hour written and 2-hour **MAPLE** lab), and one example of a student's **MAPLE** examination solutions[6]. There is a fairly full outline of my 3rd year course in **[3]**, and the complete text of that USNA conference paper is now available at **[4]**. An elementary, related paper is **[5]**.

In September 1998 the U.S. President, Bill Clinton, and the Irish Prime Minister, Bertie Ahern, engaged in a 'historic, first digital signing of a treaty on e-commerce'[7] between the U.S. and Irish governments and, motivated by that visit–which was widely reported in the media–I decided to offer a ***public*** lecture (using **MAPLE**)–***Bill Clinton, Bertie Ahern, and digital signatures***–at my college, to explain the essential ***revolutionary*** ideas of

---

[1] I got a laugh at the start of my Chicago talk by saying: *Well you all know who 'Bertie Ahern' is (he's the Irish Prime Minister), but you may not know who 'Bill Clinton' is: he's married to Senator Hilary Clinton.*

[2] Which, on downloading, may be altered by anyone who has **MAPLE**.

[3] Which may be read by anyone with internet access, who may not have **MAPLE**.

[4] To whom I dedicated my Chicago talk.

[5] And, incidentally, similar materials for other courses that I teach (second year *Number Theory*, second year *Real Number System and Cantorian Set Theory*, third year *Challenging Mathematical Puzzles and Problems*), or taught in the past (a first year, year long, course on Calculus/Analysis/**MAPLE**).

[6] My readers might be interested to know that the majority of my students are studying for the Bachelor of Education degree (preparing to be primary (elementary) school teachers), who are choosing Mathematics as one of their 'academic' subjects; they choose two such subjects in their first year of study, and continue with just one of those for their final two years.

[7] It was performed at Gateway 2000's Dublin office (Gateway's then European headquarters), and using software produced by Baltimore, the Irish cryptography company. Baltimore was then a small, ambitious outfit, which–on the back of the Clinton-Ahern signing–became the subject of a 'reverse takeover' by the much larger British cryptography company, Zergo. Baltimore's share value suddenly leaped, it made it into the FTSE 100, peaked, and flopped with the dot.com bubble burst.

public-key cryptography, that lay behind our governments' signing. The ***Irish Times***–our leading daily newspaper–publicised my talk in advance, and the editor of its (then) weekly *Computimes* page invited me to contribute an explanatory article[8] prior to my lecture. That talk–which took me about 70 mins to deliver–is available in active **MAPLE mws** format, or in **html** format in the Public and other lectures corner of my web site. My November 2003 Chicago talk–with the same title–is a much altered version of that original one[9].

An expanded version of my November 1998 *Irish Times* article.

'***Digital history made in Dublin***' was the headline (***Irish Times***, September 5th 1998) after US President Clinton and the Irish Taoiseach Bertie Ahern digitally signed a US-Irish communiqué on e-commerce using cryptographic software developed by Baltimore Technologies. Just what is a digital signature? It is a mathematically driven electronic form of a normal signature, a revolutionary development made possible through 'public-key' cryptography. How does it work?

First it is **fundamental** to appreciate the **difference** between **private**-key[10] and **public**-key cryptography and, to do so, I offer the following **idealisation** as a means of capturing the essential idea of **private**-key cryptography[11]. Imagine that you and I–who *trust* each other–have two paints, *P1* and *P2*, with these two **properties**:

Property #1. A text[12] painted[13] with *P1* by me, and sent to you, may be recovered by you by painting[14] the disguised text with *P2*. Conversely a text painted with *P2* by you, and sent to me, may be recovered by me by painting the disguised text with *P1*.

Property #2. It is understood that anyone who knows either of our paints may somehow manufacture the other one, and thus it is essential that we keep **both** paints **secret**.

A slight, but critical variation captures the essential idea of **public**-key cryptography[15] (including the novel concept of a *digital signature*). Imagine I have two paints, *P* (**public**, available to **anyone**) and *S* (**secret**, available **only** to me), with these properties:

---

[8] That Monday 16 November 1998 article–with headings '**Mathematics offers new ways of making a mark**' and '**Security: John B. Cosgrave introduces the idea of digital signatures**'–used to be freely available at the ***Irish Times*** site, but unfortunately the ***IT*** now charges for access.

[9] One significant alteration is that I include an introduction to the Pohlig-Hellman 'public-key' cryptographic method in my Chicago talk.

[10] That is *classical* cryptography, the most brilliant exposition of which is undoubtedly David Kahn's **The Codebreakers ([6])**

[11] Which I demonstrated in my Chicago talk, using the Pohlig-Hellman method.

[12] 'Plaintext' is the cryptographic jargon.

[13] 'Encrypted' is the jargon.

[14] 'Decrypted'.

[15] Proposed in the landmark 1976 paper of Diffie and Hellman, and realised in another revolutionary paper of 1978 by Rivest, Shamir, and Adleman (see **[3]** for these and other references).

Property #1a. A text painted over with *S* by me, and sent to you, may be recovered by you by painting over the disguised text with *P*. Conversely a text painted over with *P* by you, and sent to me, may be recovered by me by painting over the disguised text with *S*.

Property #2a. It is **understood** (and essential) that **nobody** who **knows** *P* can manufacture *S* (in a reasonable amount of time).

Someone can then communicate with me by writing a message on a surface, painting over with *P*, and sending the painted surface to me. On receipt, by painting over with *S*, I recover the message. Can the recipient have confidence the message came from the purported sender? No, not with this simple encryption. There is, however, a solution. Suppose the sender has paints *P1* and *S1*, with similar properties to P and S. She writes her message on a surface, and applies two disguising coats of paints: first her secret *S1*, then my public *P*. On receipt of the doubly-disguised surface I apply two revealing coats of paint: first my secret *S* (stripping the top layer), then her public *P1*, revealing the original message. In this case the sender's identity is assured by the fact that her secret paint *S1* has been used to prepare the message. For paints in the above example, substitute mathematical concepts based on large prime numbers. The precise and beautiful mathematical ideas involved–toned (but not dumbed) down–will be covered in a public lecture next week. ***Bill Clinton, Bertie Ahern, and digital signatures*** will take place in St Patrick's College, Drumcondra, Dublin, at 8 p.m. on Wednesday, November 25th. The lecture will be given by John Cosgrave of St Patrick's College, using a computer and **MAPLE** software. [end of my modified ***Irish Times*** article]

Since November 1998 I have used that public lecture to introduce my course to my students: my aim has been to show just how much one can cover with a general public audience. My third year course then entails putting ***mathematical flesh*** on that public lecture. My students have already studied Number Theory in their second year, that course consisting of three core areas: Congruences, the Euclidean Algorithm and its extension (and applications), Fermat's 'little' theorem with applications, plus other topics that I change from year to year.

Readers interested in seeing the above private-key and public key methods illustrated with text examples should access the **MAPLE** talks (the original 1998, and the Chicago) at my web site. Because I included the extra Pohlig-Hellman illustration in my Chicago talk then I didn't get to give a complete RSA demonstration in Chicago; instead I gave a modified illustration.

REFERENCES

[1] My web site homepage address is: `www.spd.dcu.ie/johnbcos`
From there follow links to **Courses I teach** (where **Exam papers** are to be found), **MAPLE, Public and other lectures**

[2] David Joyner's **Cryptography and coding theory with MAPLE page** is at:
`http://web.usna.navy.mil/~wdj/crypto.htm`

[3] Cosgrave, John: ***Number Theory and Cryptography*** (***using*** **MAPLE**) in David Joyner USNA (Ed.), Coding Theory and Cryptography: From Enigma to Geheimschreiber to Quantum Theory (Unites States Naval Academy Conference), Springer-Verlag, 2000, pp 124-143

[4] All papers from the USNA October 1998 Conference are now available from:
`http://web.usna.navy.mil/~wdj/papers/cryptoday.html`

[5] Cosgrave, John: From divisibility by 6 to the Euclidean Algorithm and the RSA cryptographic method. The American Mathematical Association of Two-Year Colleges Review. Vol.19, No 1, Fall 1997, 38-45

[6] Kahn, D.: **The Codebreakers (The Comprehensive History of Secret Communication from Ancient Times to the Internet)** (1996) Scribner