University of Waterloo Convocation Address for the Faculty of Mathematics
by Ronald L. Rivest. June 13, 2014.

Chancellor Watsa, President Hamdullahpur, Dean Goulden, members of the Faculty of Mathematics, distinguished guests, graduating students, and your families and guests.

I am pleased and honored to be here to help you celebrate!
This is a happy occasion.

So, let me be among the first to offer my congratulations to all of you who are about to graduate! You, and your families and loved ones who have supported your education, deserve to be proud of your accomplishments.

And let me thank the University of Waterloo for this honorary doctorate; I am very pleased to receive this prestigious honor from this quite young but already very stellar institution. I also like the pink tie that came with this award!

Thanks, Ian, for the generous introduction and kind words. I must confess that you missed one of my favorite accomplishments, which is the invention of ``Alice" and ``Bob". Those of you who have studied cryptography know that Alice and Bob are by now essential characters in the plot of any new cryptography paper...

I found it a challenge to prepare this convocation address; I have never given one before.

I was born perhaps four decades before you; even ten years before the founding of this University.

When I was your age, computers were new, but 10,000 times slower. Programming them was done on punched cards. The structure of DNA had just been figured out, and humans had just set foot on the moon.

While the twentieth century had many marvels, the twenty-first promises to be even greater.

You will have self-driving cars, truly intelligent computers, and grandchildren whose DNA was edited before birth. You will colonize Mars.

You will also figure out how the brain works, what the universe is really made of, how to cure cancer, and how to make fusion power work. It will be a truly exciting century. Math and computer science will play a central role in all of these developments.

What else?
Well, I had a wonderful tour of your new Quantum-Nano Center this morning. Will this century also see the development of *quantum computers*?

I must say I have very mixed feelings about this prospect!

On the one hand, it is a marvelous and ambitious scientific and engineering challenge.

On the other hand, the success of quantum computation would mean the death of many lovely cryptographic methods, including the RSA cryptosystem. On balance, I'll succumb to my biases and hope that quantum computation never succeeds! Sorry...

However, cryptographers have often seen their methods broken. Cryptography is hard, and failure is not uncommon. One must live with the truth.

Let me give two personal examples.

In 1978 we published a 129-digit RSA challenge that we thought would take 40 quadrillion years to solve. It was broken in 1994 by a new factorization algorithm implemented as a distributed computation over the Internet.

As a second example, the MD5 cryptographic hash algorithm I designed in

1991 was broken a dozen years later by Xiaoyun Wang, a Chinese researcher, using a very clever new attack algorithm.

One learns from one's failures; we now use much longer RSA keys and re-designed hash algorithms.

I have also experienced business failure. Silvio Micali and I designed the ``Peppercoin'' payment system and tried to commercialize it. While our cryptography was sound, our venture failed for lack of support from existing financial institutions.

I learned that just having the best technology is not enough; it may also need to ``fit in'' well with existing practice and infrastructure.

Today, Bitcoin seems poised to succeed in a large way, perhaps because it side-steps any dependence on existing financial institutions.

What can I say that might help *you* prepare, as you move on from Waterloo to the next stage of your lives? Have I gained any useful bits of wisdom during my own career that I could share here?

Well, cryptographers have a very interesting mind-set, which I like to call ``paranoid optimism'' (or maybe ``optimistic paranoia'').

To be a cryptographer, one has to be professionally paranoid, and to repeatedly ask ``What could go wrong?'', and ``How could an adversary, perhaps even an insider, defeat this system?''

I can recommend a healthy dose of such paranoia to you, particularly if you are designing or building new systems. Keep asking yourself ``What could go wrong?'' and ``How could a malicious adversary do harm to this system?'' Too many systems are designed today without even considering adversarial attacks.

The second aspect, ``optimism'', refers to the enormous confidence cryptographers tend to have that, once a potential attack is identified,

cryptographic methods can be invented or adapted to counter the new attack.

And, historically, this is case: we now have cryptographic methods of incredible subtlety and power that enable one to do amazing things, such as proving to someone else that you know a solution to a problem without giving them any idea as to what the solution actually is, or being able to verify that your vote was correctly counted, without being able to prove to anyone else how you voted.

So, I encourage you to adopt a bit of ``paranoid optimism" in your approach to life. Keep a paranoid eye out for what could go wrong, but be optimistic that you can overcome adversity and failure and make things work out well in the end.

I have three other bits of advice for you before I close.

(1) *Keep a broad perspective.* Alan Kay once said,
``Having the right point of view is worth 80 IQ points."
To illustrate this, let me recommend meditation on
the following mind-expanding quote from the late Steve Jobs:
"Life can be much broader once you discover one simple
fact---everything around you that you call life was made up
by people that were no smarter than you."

(2) *Work hard.* Reward is at least quadratic in your effort.
Many activities are actually characterized by ``increasing returns".

(3) *Stay curious.* The most important thing about the degree you are about to receive is not that you know something, but that you
you've learned ``how to learn." The world changes fast,
and is full of wonderful things. Keep learning.

Let me finish by saying, "Graduates, congratulations again to you, your mentors, and your families!" Celebrate tonight, then tomorrow move on with pride and confidence! After, of course, changing all of your passwords!