R.N. 70269/98
ISSN : 0972-169X

Postal Registration No.: DL-SW-1/4082/12-14
Date of posting: 26-27 of advance month
Date of publication: 24 of advance month

Vigyan Prasar

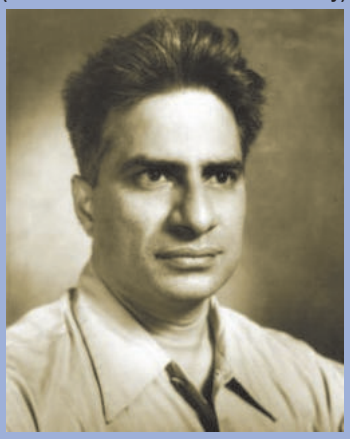
DREAM 2047

June 2013 Vol. 15 No. 9 Rs. 5.00

Mathematics of Planet Earth 2013

A Chronicle of Cryptography

Damodar Dharmanand Kosambi
(A Scientist with Renaissance Versatility)



(1907-1966)

... think scientifically, act scientifically... think scientifically, act scientifically... think scientifically, act...

Sector-specific and cross-sectoral science and technology information support and capacity building interventions

Dr. R. Gopichandran

A recent working paper from the Madras school of Economics (Sankar U, 2012) highlighted the need to establish knowledge sharing synergies between scientists and economists. This was with special reference to aspects of sustainable development that have to be mainstreamed into public policy frameworks. The author draws attention to Amartya Sen's deliberation on scientific temper integrating logic, reason and notions that are not biased/pre-conceived. He further refers to Pandit Jawarharlal Nehru's perspective on scientific temper. In this context an important reference to four important indicators of economic growth as a function of technical progress sets the context for specific science and technology interventions. They include higher production aligned with efficient appropriate material and energy input-output proportions and discovery/use of alternative materials and production systems. These aspects are integral also to eco-industrial development.

Importantly, principles of preventive environmental management are embedded in such perspectives and can help fulfil immediate goals set by the various sector-specific missions of our country for the present 12th Plan period as a priority. Citizens as consumers of products and services can influence sustainable production and consumption and help reduce the spread and depth of externalities. Sankar (*op. cit*) accordingly reinforces the need for cross sectoral linkages based on a clear understanding of challenges and options to overcome them. A recent working paper by Bryant and Goodman (2013) provides interesting insights on the dynamics of involving citizens in sustainable production and consumption practices. The need to deliver appropriate scientific and technical information to assist well adapted public policies that will assist large scale transitions is highlighted also by the James A Baker III Institute of Public Policy (2013) of the Rice University.

Michael Clegg (2012) the Co-Chair of Inter-American Network of Academies of Science recently defined the unique values of science and scientific approach duly recognising its pervasive nature across thrust areas relevant for sustainable development. In this context he rightly highlighted scientific temper as a means of enhancing tolerance and rationality. These attributes of understanding world views of development will help citizens comprehend emerging and continually evolving facets of knowledge.

References

1. Sankar U (2012) Science and Economics for Sustainable Development of India Working Paper 76/2012; 29p. Madras School of Economics, Chennai http://www.mse.ac.in/pub/WORKING%20PAPER%2076.pdf
2. Bryant R & Goodman MK (2013) Environment, Politics and Development Working Paper Series No 55. 19p. Department of Geography, King's College, London. http://www.kcl.ac.uk/sspp/departments/geography/research/epd/BryantWP55.pdf
3. James A Baker III Institute of Public Policy (2013) Policy recommendations for the Obama Administration. 108p. http://www.bakerinstitute.org/publications/BI-pub-PolicyRecommendations-021313.pdf
4. Clegg M (2012) Science for Global Development: The Role of Networks of Science Academies http://www.fapesp.br/eventos/2012/08/FMC/Michael_Clegg.pdf

Email: r.gopichandran@vigyanprasar.gov.in ■

Editor : Subodh Mahanti
Associate editor : Rintu Nath
Production : Manish Mohan Gore and Pradeep Kumar
Expert member : Biman Basu
Address for correspondence : Vigyan Prasar, C-24, Qutab Institutional Area, New Delhi-110 016
Tel : 011-26967532; Fax : 0120-2404437
e-mail : info@vigyanprasar.gov.in
website : http://www.vigyanprasar.gov.in

Published and Printed by Dr. Subodh Mahanti on behalf of Vigyan Prasar, C-24, Qutab Institutional Area, New Delhi - 110 016 and Printed at Aravali Printers & Publishers Pvt. Ltd., W-30, Okhla Industrial Area, Phase-II, New Delhi-110 020 Phone: 011-26388830-32.

Damodar Dharmanand Kosambi
A Scientist with Renaissance Versatility

Dr. Subodh Mahanti
E-mail: smahanti@vigyanprasar.gov.in

"Professor D.D. Kosambi was endowed with a truly renaissance versatility. He was one of the few great Indians who grasped the nature of twentieth century science and technology and its implications for humanity. Shunning the limelight of publicity, he made outstanding contributions to various fields of knowledge, which included mathematics, statistics, numismatics, Indology, history as well as contemporary social problems. He devoted a great deal of his time to the Peace Movement and campaign against nuclear weapons."

Arvind Gupta in *Bright Sparks: Inspiring Indian Scientists from the Past,* 2009

"The guiding principle in all his (D.D. Kosambi's) activities was his love for humanism and peace. His approach to life was based on Marxism but not its blind uncritical application. He used to mix freely with all the cross sections of the community to understand their problems, as according to him this was the first step to solve problems in science…He was intensely human with natural compassion for the fellow human being, especially for the underdog and he championed their cause with all vigour and strength."

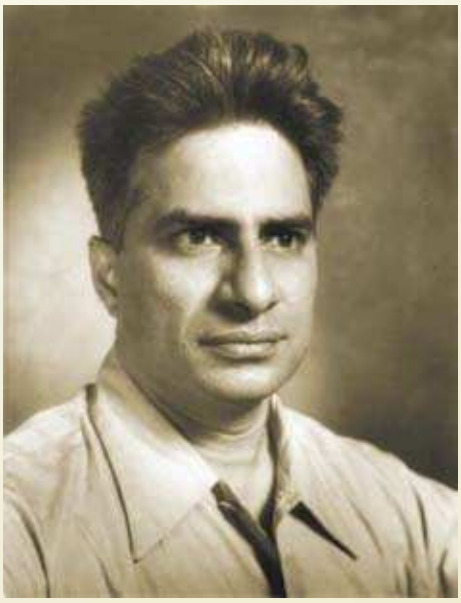
P.V. Sukhatme in *Biographical Memoirs of Fellows of the Indian National Science Academy* (Vol.18), 1994.

"He (D.D. Kosambi) was a larger than life personality, and even his personal life was an important statement. His integrity—personal and intellectual—was beyond question. Secularism formed the core of his personality. He made no distinction based on religion, caste, race, or gender, and brought up his children with the same secular ideology. He has always had a unique, international identity as a brilliant, profound and original scholar straddling many fields of knowledge. And this identity will endure as long as scholarship itself endures."

Meera Kosambi in *Resonance*, June 2011.

Damodar Dharmanand Kosambi made significant contributions to diverse fields of human knowledge. He made notable contribution to the development of higher mathematics and statistics. He published research papers in Indian and international journals in pure and applied mathematics and statistics. P.V. Sukhatme has described Kosambi's fascination with mathematics: "He (Kosambi) had only a Bachelor's degree in mathematics and yet had a complete grasp over the latest developments in mathematical research in Europe. He regarded mathematics as the language of nature, giving preciseness to the results of other sciences, but was also aware that nature has its own philosophy. He was very much fascinated by the clarity and exactness which mathematics can give and brought to bear the same in all branches of science he handled." In mathematics he mostly worked in tensor analysis and path-geometry, a term he himself coined. He also worked in theoretical and nuclear physics.

Kosambi's formula for finding the distance between chromosomes was considered as a significant contribution to classical genetics. As pointed out by Sukhatme, his formula 'gave satisfactory additive estimates of map lengths irrespective of the kinds of organisms and the lengths of their chromosomes on which recombination data are gathered.'



Damodar Dharmanand Kosambi

Through his extensive and painstaking work on Indian coins he established the science of coins or numismatics as an exact scientific branch.

He was the first to recognise the presence of microliths characteristic of the Stone Age on the Vetal Plateau on the Western Ghats. He discovered several trade routes. Based on his extensive field work he suggested the use of Malshej Ghat, a mountain pass in the Western Ghats range in Pune district, as a key road from Mumbai to Ahmedanagar. It was Kosambi, who first deciphered the Brahmi inscript at the Karla Caves, a complex of ancient Indian Buddhist rock-cut cave shrines located in Karli near Lonavala in Maharashtra.. He discovered many Neolithic routes, Buddhist caves, and old inscriptions. He established the Archaeology Society and donated his rare collections to its museum.

Kosambi threw light on the most vital missing link in the Robert Graves' researches on the life of Christ by establishing the presence of Christ in Kashmir from some rare documents in Srinagar Fort. He developed a new interpretation of Indian history. His classic works on Indian history marked a new stage in Indian historiography.

Kosambi was a great linguist. He learnt Sanskrit, Brahmi and Prakrit languages. He also studied several European languages, viz., French, German, Italian, and Russian. He had enough working knowledge in Latin, Greek, and Hebrew.

Kosambi was an active participant in the activities undertaken by the World Peace Council. He led the Indian delegation to the World Peace Conference held at Helsinki in June 1955. The Helsinki Conference was chaired by the French physicist and a Nobel Laureate Frederic Jolliot-Curie and among its participants were J.D. Bernal and Jean-Paul Sartre.

Kosambi was born on 31 July 1907 in village Kosben in Goa. His father Dharmanand Kosambi was a renowned Buddhist scholar. Dharmanand Kosambi, who taught Pali at the Fergusson College, Pune was also a Visiting Faculty of the Harvard University, USA. Kosambi had his early schooling in Pune. In 1918, Kosambi and his sister went to Cambridge, USA along with his father, for whom it was a second visit to Harvard University. Kosambi first enrolled in the Cambridge Grammar School and later studied at the Cambridge Latin School. After four years his father and his sister returned to India but Kosambi had to stay back to complete his schooling. Eventually he came back to India after completing his school education and he wanted to continue his education in India. However, he failed to get admission in any college in India because the school educational system of USA was not compatible with the Indian system. So, after spending a year he returned to Cambridge, USA and joined Harvard University. In 1929, Kosambi graduated from Harvard University with distinction (*summa cum laude*). Kosambi wanted to pursue his doctoral studies at Harvard, but he could not manage financial support because in view of the on-going economic depression it was extremely difficult to get a scholarship.

J.D. Bernal

Jean-Paul Sartre

Dharmanand Kosambi

In 1929, Kosambi came back to India and joined Banaras Hindu University as Professor of Mathematics. At BHU, where he stayed for about two years, he also taught German language in addition to mathematics. From BHU, he went to Aligarh Muslim University (AMU), at the invitation of Andre Weil, the French mathematician who was heading the Department of Mathematics. He stayed at AMU for about a year. In 1933, Kosambi joined the Ferguson College in Pune, where his father once worked. He served the Fergusson College for 14 years. Meera Kosambi wrote: "In 1933 he (Kosambi) joined the faculty of the Fergusson College at Pune. Here he became known as an exacting professor, not easy to understand and not popular with those who expected to be spoon-fed, but highly admired by the bright and serious students who were willing to work hard." He resigned from the college because of his differences with college authorities. He was not happy with the 'examination-ridden system and uninspiring standards of education.'

Andre Weil

On being invited by Homi J. Bhabha, Kosambi joined the newly established Tata Institute of Fundamental Research (TIFR), Mumbai in 1946. Initially he had a very cordial relationship with Bhabha. However, because of his aversion to nuclear energy and fierce independent mind his relation with Bhabha worsened. In 1962, Kosambi left TIFR as his contract was not renewed.

In 1949, he was a visiting professor at the University of Chicago in USA, where he taught path-geometry. He was a guest at the Institute of Advanced Study at Princeton, where he took part in extensive discussion with Albert Einstein on theory of relativity. In 1964, Kosambi was appointed scientist emeritus by the Council of Scientific and Industrial Research (CSIR) and he was affiliated to the Maharashtra Association for the Cultivation of Science, Pune.

While studying old Indian coins Kosambi developed an intellectual urge to know about the kings who struck the coins and he realised that this could be done only with a fairly good knowledge of Sanskrit literature. He had no formal training in Sanskrit literature, but he had some knowledge of it through informal studies with his father. So he decided to study Sanskrit literature in a systematic way. He began with Bhartrihari's three *Shatakas* of epigrams. He found Bhartrihari's text defective and he undertook text-criticism.

Ferguson College in Pune

He studied about 400 manuscripts within a span of five years. He not only revived the works of over 50 poets who went into oblivion but also added to the knowledge of works of other lesser-known poets. He prepared a critical edition of the poetry of Bhartrihari (The *Sataka-trayam* of Bharthrihari with the commentary of Ramarsi) edited in collaboration with Pandit K.V. Krishnamoorthi Sharma, 1945). After Bhartrihari's *shatakas* he took up the Sanskrit literary anthology *Subhashita-ratna-kosha* (The *Subhasita-ratna-kosa* of Vidyakara edited with V.V. Gokhale). Vidyakara's anthology is the oldest example of Sanskrit literature. These works are considered landmarks in text criticism. Sheldon Pollock wrote: "Two traits, as an ensemble, distinguish D.D. Kosambi in his work on Sanskrit not only from the scholars who were his contemporaries, but also from almost everyone since. The first is his search for method in the editing of Sanskrit literary texts, and the second his search for a theory in reading of these texts. In the former case, if judged by the practices of editing Sanskrit literary texts in India at the time, Kosambi emerges as a remarkable pioneer, his concrete accomplishment hardly in danger of being superseded anytime soon. In the latter, he is exceptional in the history of Indology for his awareness that the method of philology is always inseparable from a theory of philology, itself produced by a tradition of writing and reading, and from a cultural and political criticism specific to that tradition. If Kosambi's theory has proven to be flawed, we have only come to know the flaws and sought ways to overcome them because he had the courage to enunciate the theory in the first place."

Homi J. Bhabha

Kosambi was attracted to Indian history while he was studying Sanskrit literature. He redefined the nature and scope of Indian history. Meera Kosambi wrote: "Kosambi is credited with having wrought a revolution through his redefinition of the nature and scope of history. For one thing, he dismantled the entrenched notion of fixed periods—Ancient, Medieval and Modern periods of Indian history. For another, he designed an integrated methodology for harnessing diverse sources. In his famous and seminal essay—which he labels as 'note'—entitled 'Combined Methods in Indology', he critiques the practice of placing sole reliance upon linguistic sources." Sukhatme wrote: "He found that no reliable sources of data exist and arrived at a new definition of history, adopting it from the theory of Karl Marx. According to Prof. Kosambi, history should be related to the development of means of production and that farmers, villagers, low-caste nomads, tribal minorities were the main sources of data for writing history as distinct from a series of historical episodes relating to kings." Realising the fact that written words would not suffice, he engaged himself in studies in archaeology and ethnography and made significant contributions in these fields. For Kosambi history was not a subject which dealt only with the dead past. For him history lived on in the present.

He brought in fundamental insights in understanding the nature of Indian feudalism and this led several scholars to study the feudal structure of Indian society and state. His major works on Indian history namely, *An Introduction to the Study of Indian History* (1956), *Myth and Reality: Studies in the formation of Indian culture* (1962), *The Culture and Civilisation of Ancient India in Historical Outline* (1965) became a must reading for researchers and students of history both in India and abroad. These works have been translated into several foreign languages.

Kosambi's writings on history evoked great admiration as well as well as severe criticism. Thus Meera Kosambi wrote: "This extensive re/writing of history (by D.D. Kosambi) elicited the expected and contradictory responses. He was praised by some as a pioneer of genuine Marxist scholarship of the Indian past and demonised by others as a nasty iconoclast using an alien framework inappropriate for the study of Indian cultural heritage."

Kosambi was the recipient of the first Ramanujan Memorial Prize (1934). He also won a special Bhabha Prize in 1947. He was elected a Fellow of the Indian National Science Academy, New Delhi.

Kosambi died on 29 June 1966 at the age of 58.

Based on Kosambi's way of looking at Indian history, Arvind Narain Das, a well-known activist and social scientist produced a 13-episode serial titled "India Invented" in the early 1990s. In 2008, the Department of Post, Government of India issued a postal stamp in memory of Kosambi. A Kosambi Chair has been established at the University of Pune.

Kosambi worked in diverse fields—mathematics, statistics, physics, numismatics, genetics, Sanskrit literature, history, and archaeology and made significant contributions. He not only raised significant new questions but also offered original answers. We would like to end this article by quoting Meera Kosambi: "Kosambi's astounding intellectual journey effectively demonstrates the meaninglessness of disciplinary boundaries and the insistence on formal training and degrees as the only marker of knowledge."

References

1. Gupta, Arvind, *Bright Sparks: Inspiring Indian Scientists from the Past*, New Delhi: Indian National Science Academy, 2009.
2. Kosambi, Meera, "D.D. Kosambi: The Scholar and the Man", *Resonance*, pp.501-513, June 2001.
3. Pollock, Sheldon, "Towards a Political Philosophy: D.D. Kosambi" and Sanskrit, *Economic and Political Weekly*, pp.52-59, July 26, 2008.
4. Sukhatme, P.V., "Damodar Dharmanand Kosambi (1907-1966)" in *Biographical Memoirs of Fellows of the Indian National Science Academy* (Vol.18), New Delhi: Indian National Science Academy, 1994.
5. Available sources on the Internet.

(*The article is a popular presentation of important points on the life and work of* Damodar Dharmanand Kosambi *available in the existing literature. The idea is to inspire younger generation to know more about Kosambi. The author has given sources consulted for writing this article. However, the sources on the Internet have not been individually listed. The author is grateful to all those writings have contributed to writing this article.)* ■

A Chronicle of Cryptography

Rintu Nath
E-mail: rnath@vigyanprasar.gov.in

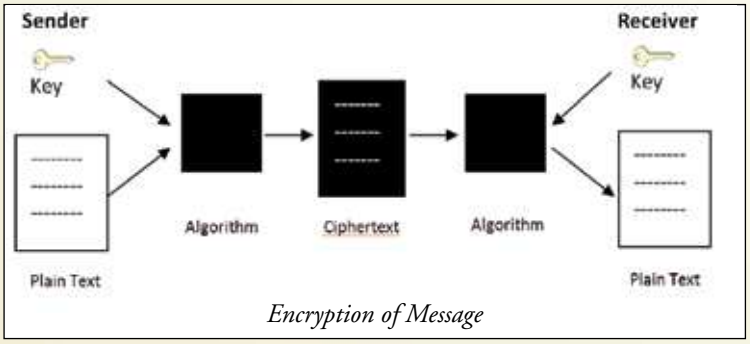
Information is becoming an increasingly valuable commodity in modern society. With the revolution in communication systems, the exchange of information has become very efficient, obliterating the limits of geographic location or time. However, for services like Internet banking, mobile banking, security services, etc., the exchange of data through the existing communication network is not adequate. It is essential that the exchange of data for these services is carried out with utmost confidentiality and securely without unauthorised access or interception. Only an established secured mode of communication technique can ensure the integrity of the data.

In most of the cases, information travels through interconnected heterogeneous communication networks, managed by different organisations. Hence, providing physical security to a communication network may not be feasible. Interception of the data from apparently secured communication channel is possible. Hence the aim is not to hide the existence of a message, but rather to hide its content, a method known as encryption. In encryption, a message is scrambled according to a particular protocol and an encryption key, which is agreed beforehand between the sender and the intended recipient. Thus the recipient can reverse the scrambling protocol using the key and make the message comprehensible. Without knowing the scrambling protocol and the key, the unauthorised person would find it difficult, if not impossible, to re-create the original message from the encrypted text. Hence, in the event of an unauthorised access, the encrypted message will not be understood by the unauthorised person. The security of the message is thus essentially dependent on the strength of the encryption algorithm.

Data encryption is not a modern phenomenon. Practice to hide secret information can be traced back to the fifth century BC. Historically, many kings, queens and generals relied on sending and intercepting secret information. Data encryption and decryption played an important role in the two World Wars. New techniques to encrypt information evolved with the development of the telegraph, radio, computer and Internet. Handwritten cipher was replaced by machine cipher. In fact, the urge to develop complex code for encryption and decryption led to the development of the computer.

The aim is not to hide the existence of a message, but rather to hide its content, a method known as encryption

Cryptography is the practice and study of different techniques and algorithm of encryption. The word *crypto* is derived from the Greek *kryptos*, meaning "hidden". Early cryptography was solely concerned with converting messages into unreadable groups of figures to protect the message's content while the message was being carried from one place to another. Modern cryptography, however, in addition to encryption, also deals with message integrity checking and sender/receiver identity authentication.



Encryption of Message

The evolution of secret writing

Historically rulers have relied on secret communication in order to govern their provinces and command their armies. At the same time, they were all aware of the consequences of their messages falling into the wrong hands, revealing precious secrets to rivals. It was the threat of enemy interception that motivated the development of codes and ciphers: techniques for disguising a message so that only the intended recipient can read it.

It was the threat of enemy interception that motivated the development of codes and ciphers

Secret communication achieved by hiding the existence of a message is known as 'steganography', derived from the Greek words *steganos*, meaning "covered," and *graphein*, meaning "to write." Steganography also includes the practice of writing in invisible ink. The method suffers from a fundamental weakness: If the message is discovered, then the contents of the secret communication are revealed at once. Interception of the message immediately compromises all security.

Caesar cipher

The first documented evidence of using cryptography was by Julius Caesar. Caesar used to send written instructions to the war front. Instead of trying to send the message secretly, he chose an innovative method by which he could hide the meaning of the message. Even if the messenger was captured by his enemy, they would not be able to understand the meaning of the message that the messenger was carrying. He simply replaced each letter in the message with the letter that is three places further down the alphabet. To honour him for inventing this form of encryption, it is known as *Caesar shift cipher* or simply *Caesar cipher.*

In terms of cryptography, the letters used to write the original message are called *plain alphabet* and the letters substituted in place of plain letters are called *cipher alphabet. Messages written using plain alphabets* are called *plain text* and when *plain alphabets* are replaced by *cipher alphabets,* it is called *cipher text.*

In Caesar cipher, if cipher alphabets are placed below the plain alphabets, it becomes clear that cipher alphabets are shifted by three places.

If the original message is "attack in the morning", in

Plain alphabet	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
Cipher alphabet	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caesar cipher: cipher alphabets are shifted by three places

Caesar cipher, its cipher text will be "dwwdfn lq wkh pruqlqj". Clearly the cipher text is not decipherable.

This form of generation of cipher text is known as *substitution cipher*, where each alphabet is replaced by another predetermined alphabet. Although Caesar cipher shifts three places, it is clear that any number of shifts between 1 to 25 is possible is possible to generate a cipher text.

Drawback of this system is that this code can be broken easily. With the knowledge of substitution cipher and with the help of different permutation and combinations, this can be broken in no time.

Sometime a key is used in the substitution cipher. For example, to use "DREAM" as a key, it will be used at the beginning of the cipher alphabet. The remainder of the cipher alphabet are merely the remaining letters of the alphabet, in their correct order, starting where the key ends and not repeating the alphabets used once in the key.

While the cryptographer develops new methods of secret writing, it is the cryptanalyst who struggles to find weaknesses in these methods in order to break into secret messages.

Plain alphabet	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
Cipher alphabet	D	R	E	A	M	N	O	P	Q	S	T	U	V	W	X	Y	Z	B	C	F	G	H	I	J	K	L

Caesar cipher with key 'DREAM'

"attack in the morning" will be now coded as 'dffdet qv fpm vxbwqwo".

An enemy studying an intercepted scrambled message may guess that each alphabet is replaced by another, however, without the knowledge of the key, "DREAM" in this case, it would be very difficult to reconstruct the original message.

This method of replacing a letter by another is known as 'mono alphabetic substitution cipher'.

Cryptanalysis

Documentary evidences suggest that during the ninth century, Arabic scholars not only used mono alphabetic substitution cipher technique to encrypt message, they also knew how to decrypt without any knowledge of the key. They in fact invented 'cryptanalysis', the science of unscrambling a message without knowledge of the key. While the cryptographer develops new methods of secret writing, it is the cryptanalyst who struggles to find weaknesses in these methods in order to break into secret messages.

Arabian cryptanalysts succeeded in finding a method for breaking the mono alphabetic substitution cipher, a cipher that had remained unbreakable for several centuries.

One of the methods employed to break mono alphabetic substitution cipher is to use frequency analysis. In English, 'e' is the most common letter, followed by 't', then 'a', and so on as given in the table 1.

A cryptanalyst can do a frequency analysis of a cipher text and based on the frequency of letters he/she can replace the most probable letter from table. For example, if a cipher text contains maximum number of 'k', it is quite possible that during the encryption letter 'e' was replaced by 'k'. Similarly other letters can also be replaced based on the frequency of their occurrence.

However, it is not possible to apply frequency analysis for cryptanalysis unconditionally, because the standard list of frequencies in Table 1 is only an average, and it will not correspond exactly to the frequencies of every text. Moreover, frequency analysis is only applicable if cipher text length is sufficiently large. However, the method proved to be quite useful in decrypting many secret codes during the tenth century.

Table 1

Letter	Percentage	Letter	Percentage
A	8.2	**N**	6.7
B	1.5	**O**	7.5
C	2.8	**P**	1.9
D	4.3	**Q**	0.1
E	12.7	**R**	6.0
F	2.2	**S**	6.3
G	2.0	**T**	9.1
H	6.1	**U**	2.8
I	7.0	**V**	1.0
J	0.2	**W**	2.4
K	0.8	**X**	0.2
L	4.0	**Y**	2.0
M	2.4	**Z**	0.1

This table of relative frequencies is based on passages taken from newspapers and novels, and the total sample was 100,362 alphabetic characters. The table was compiled by H. Beker and F. Piper, and originally published in *Cipher Systems: The Protection of Communication.* [credit: *The Code Book* by Simon Singh]

As cryptanalysts started breaking secret codes using frequency analysis during the tenth century, 'poly alphabetic substitution method' was invented, where two similar letters in the plain text may be represented by two different letters in the cipher text.

Transposition

There is another form of cryptography, known as transposition. In transposition, the letters of the message are simply rearranged, effectively generating an anagram. For very short messages, such as a single word, this method is relatively insecure because there are only a limited number of ways of rearranging a handful of letters. For example, three letters can be arranged in

only six different ways, e.g., rat, tar, atr, tra, rta, art. However, as the number of letters gradually increases, the number of possible arrangements rapidly explodes, making it impossible to get back to the original message unless the exact scrambling process is known. In a 'transposition cipher', spaces in between words are omitted. Therefore, "attack in the morning" can be jumbled-up to "intheackattningmor". There can be billions of combination that transposition cipher will offer, and hence it will be very difficult to get the meaning unless the method of transposition is known.

Rail fence transposition

In order for transposition to be effective, the rearrangement of letters needs to follow a straightforward system, one that has been previously agreed to by sender and receiver but kept secret from the enemy. For example, it is possible to send messages using the "rail fence" transposition, in which the message is written with alternating letters on separate upper and lower lines. The sequence of letters on the lower line is then tagged on at the end of the sequence on the upper line to create the final encrypted message. For example:

A	T	T	A	C	K		I	N		T	H	E		M	O	R	N	I	N	G

⇓

A		T		C		I		T		E		O		N		N	
	T		A		K		N		H		M		R		I		G

⇓

A	T	C	I	T	E	O	N	N	T	A	K	N	H	M	R	I	G

Rail fence transposition

However, this method of encryption is rudimentary and can be broken easily. An enemy studying an intercepted scrambled message may guess that alphabets are rearranged. With the help of different permutations and combinations, this encryption can also be broken.

The Vigenère cipher

For centuries, the simple mono-alphabetic substitution cipher had been sufficient to ensure secrecy. The subsequent development of frequency analysis destroyed its security. Cryptographers wanted to develop a stronger cipher, something that could outwit the cryptanalysts.

In the year 1563, Blaise de Vigenère, a French diplomat, invented a coherent and powerful new cipher, now known as the Vigenère cipher. The strength of the Vigenère cipher lies in its use of not one or two but twenty-six distinct cipher alphabets to encrypt a message. The great advantage of the Vigenère cipher is that it is invulnerable to the frequency analysis. The cipher was considered unbreakable. However, the British cryptanalyst Charles Babbage broke Vigenère cipher in the year 1854.

> Using a computer to encipher a message provided greater flexibility in terms of number of combinations in generating a key and the speed of operation

The new era of cryptography

Since Babbage had destroyed the security of the Vigenère cipher, cryptographers were searching for a new cipher, something that would re-establish the secret communication. Meanwhile, communication through telegraph started during late 18th century. Businessmen and military wanted to utilise the instancy of the telegraph without their communications being stolen and deciphered. Furthermore, during the 19th century an even more powerful form of telecommunication, radio communication was invented. This made the need for secure encryption even more pressing.

> At the outbreak of the Second World War the German military's communications were protected by an unparalleled level of encryption.

The ease of communication and ease of interception of radio signals heralded a mixed blessing for the cryptographers and thus cryptography was brought into sharp focus at the outbreak of the First World War. Radio signals travel in all directions and reach receivers wherever they are located. Therefore messages will inevitably reach the enemy as well as the intended recipient. Consequently, reliable encryption became a necessity. If the enemy was going to be able to intercept every radio message, then cryptographers had to find a way of preventing them from deciphering these messages.

During the First World War, cryptographers developed several new ciphers, but all were broken. It was Germany that suffered most from these security breaches. Cryptanalyst of the Allied forces could intercept and decipher almost all the secret radio communication of the German forces.

Enigma

In the years following the war, there was a concerted effort to find new and secure encryption systems. Cryptographers turned to technologies to help guarantee the security. Rather than relying on pencil-and-paper based ciphers, they focussed their attention on the mechanisation of secrecy.

In 1918, the German inventor Arthur Scherbius and his close friend Richard Ritter developed a cryptographic machine called *Enigma*. Scherbius patented his cipher machine in 1918. *Enigma* was contained in a compact box measuring only 13.5 inches × 11 inches × 6 inches (34.3 cm × 27.94

cm × 15.2 cm) and it weighed about 11 kg.

Scherbius' invention provided the most secure system of cryptography in the world, and at the outbreak of the Second World War the German military's communications were protected by an unparalleled level of encryption. Encryption using *Enigma* was based on polyalphabetic substitution method. Security of the encrypted message was based on the secret key. To provide added security, everyday there used to be a new key, called 'day key'. Due to frequent change in the encryption key, cipher text generated by *Enigma* was almost impossible to break with conventional methods. However, in 1932 Polish mathematician and cryptologist Marian Rejewski could devise a method to break the codes generated by *Enigma* machine.

During World War II, Alan Turing, a British mathematician, devised a number of techniques for breaking German ciphers, including the method of the *bombe*, an electromechanical machine that could find settings for the *Enigma* machine. In fact, Turing's research in the field of cryptography finally gifted the world the 'Turing machine', which can be considered a model of a general purpose computer.

Finally, In 1945, ENIAC (Electronic Numerical Integrator and Calculator), world's first computer, was developed. ENIAC was capable of performing five thousand calculations per second.

Using a computer to encipher a message provided greater flexibility in terms of number of combinations in generating a key and the speed of operation. As a computer uses binary number system, interception of any message will only provide streams of '0' and '1', thus making it extremely difficult to break the code.

In 1977, while working in the MIT Laboratory for Computer Science, Ronald Rivest, Adi Shamir and Leonard Adleman created the RSA algorithm using the concept of prime factors. RSA stands for the initials of the inventors' surnames. RSA algorithm is one of the most robust algorithms in e-commerce applications as of now. In fact, Public Key Cryptosystem, widely used in today's e-commerce applications uses RSA algorithm to generate keys.

It is estimated that even billion years is not sufficient to break RSA algorithm with all the computing power of the world put together.

The future

The exchange of digital information has become an integral part of our society. Every day millions of e-mails are sent and received. At every moment, the economy of world is being managed online where trillions of dollars are moving around. Critically, the success of all electronic transactions depend on the ability to protect information as they flow around the world, and this is only possible through the power of cryptography. Encryption can be seen as providing the locks and keys of the Information Age. For many years requirement of encryption was limited to government agencies and military. However, now every common man is directly or indirectly dependent on this important branch of science.

Quantum cryptography is based on quantum physics, a theory that explains how the universe operates at the most fundamental level.

The invention of public key cryptography using RSA algorithm provides unparalleled security. It is estimated that even billion years is not sufficient to break RSA algorithm with all the computing power of the world put together. Previous experience, however, tells us that every so-called unbreakable cipher has, sooner or later, succumbed to cryptanalysis. The Vigenère cipher was called unbreakable cipher, but Babbage broke it; *Enigma* was considered invulnerable until its weaknesses were revealed. Does it mean cryptanalysts on the verge of another breakthrough? Only time will tell us.

In 1984, Charles Bennett, a research fellow at IBM's Thomas J. Watson Laboratories in New York, developed the idea of quantum cryptography, an encryption system that is absolutely unbreakable. Quantum cryptography is based on quantum physics, a theory that explains how the universe operates at the most fundamental level. Bennett's idea is based on an aspect of quantum physics known as Heisenberg's uncertainty principle, which states that it is impossible to measure something with perfect accuracy because the act of measurement alters the object being measured. However, quantum cryptography is still in its early stage and further research is going on to implement the idea in daily transactions.

Sources

Simon Singh, The code book : how to make it, break it, hack it, crack it, Delacorte Press, New York

David Kahn, The Codebreakers: The Story of Secret Writing, Macmillan

An excellent account on history and chronology of cryptography may be found at: http://en.wikipedia.org/wiki/Cryptography

Follow your own curiosity
Interview with Anthony James Legget

Sir Anthony James Legget, popularly known as Tony Legget in the scientific community, is a leading scientist in the field of low-temperature physics. He has widely contributed to understanding the normal and super-fluid liquid helium and strongly-coupled superfluids. He has also deep interest and insight in testing the foundations of quantum mechanics using condensed systems. His pioneering work in the field of superfluidity was recognised by the award of the Nobel Prize in Physics in 2003. He is an honorary fellow of Institute of Physics (UK). He was knighted in 2004 "for services in physics". He is also a Fellow of the Royal Society.

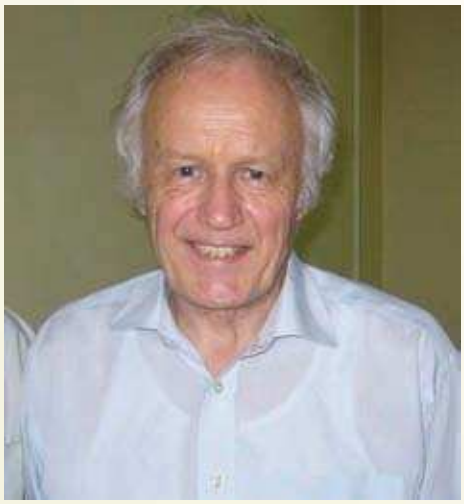
Legget was born on 26 March 1938 in a small town Camberwell, south of London in England. Legget won a scholarship from Oxford University in 1954 to study classics. After completing the degree, in the early summer of 1958, he applied to do a second Oxford undergraduate degree, in physics. After completing his academics, he did his Ph.D. on "Some Problems in the Theory of Many-Body Systems", with Prof. Dirk ter Haar at Magdalen College, Oxford. His theoretical understanding of physics took shape here and blossomed. After completing his post-doctoral studies, he accepted an offer from the University of Illinois at Urbana-Champaign (UIUC) of the MacArthur Chair, in the spring of 1982.

Meher Wan had an opportunity to listen to Sir Anthony, who delivered an invited lecture in Physics Department, University of Allahabad some years back. Here are the excerpts of an interview with Sir Anthony that Wan conducted through e-mail.

Meher Wan: Let me thank you on behalf of our readers for accepting my request for an interview on your research, life and philosophy. Your pioneering research work on super-fluidity was considered for the Nobel Prize in Physics in 2003. How has your life changed after becoming a Nobel laureate? What kind of relief or responsibility do you feel after winning this prestigious prize?

Prof. A.J. Legget: There are many ways in which my life has changed. I get more invitations than previously to give popular talks, etc., and more people want me to write letters of recommendation for them. Most interestingly, I am continually being pressed to express in public opinions on matters of which I do not know enough to have an informed opinion.

M.W.: Let us peep in to your childhood. How do you remember your school days and Beaumont? Were you extraordinarily brilliant in your school, or you achieved these successes by merely chasing your curiosity and intent for the quest of nature?



Sir Anthony James Legget

A.J.L.: Well, I remember that they used to give prizes for the best performance in about eight different academic subjects, and one year I got the prizes in all eight, which I believe was unprecedented. So I suppose that I did have a reputation for outstanding academic ability.

M.W.: At your times in schools, one had to choose science or classics or arts as stream of study in his/her very early stage of studies. When you came to Allahabad, India in a Science Conclave, you revealed that primarily you have chosen classics and literature as your study majors. What were the reasons for choosing classics and not science, when your father was a science teacher?

A.J.L.: Actually, I think my father was steeped in the attitude which was common in Britain at that time (the early fifties, pre-Sputnik), namely that classics was the most "prestigious" subject and science right at the bottom of the pecking order. Certainly he was quite happy to see me go into classics.

M.W.: After spending five years studying classics, what was the motivating force for opting for science and especially physics?

A.J.L.: Actually it was a good deal more than five years (about 5 at high school, then 4 at Oxford, if you count the part spent on ancient history and philosophy). The reason for my shift was, first, I was too unimaginative to think about any career other than an academic one, and secondly, I became convinced that, rather than working in a subject such as philosophy, where there seems to be no clear objective criteria of what constituted good work or bad, I wanted to work in a discipline where Nature herself could prove me right or wrong.

M.W.: How did the study of classics help in your further career? Did you imagine at that time, that you will do so well in physics after spending so much time in other subjects?

A.J.L.: I realised that my comparative age was some disadvantage, but I felt that my experience of studying philosophy, in particular, might compensate for this. And indeed I have found it extremely helpful, in particular in that I suspect I am much more skeptical than many of my colleagues about the "established" wisdom and the reasoning behind it.

M.W.: At the time of your post-doctoral work in University of Illinois, John Bardeen and some other impressive experimental physicists were working there. How did they influence you in the process of being a better researcher?

A.J.L.: Like many others, I did not find John the easiest person in the world to talk to, but he and Leo Kadanoff played a crucial role in my career by suggesting the problem which led indirectly to my work on superfluid Helium-3. I got more out of my interactions with David Pines (my formal postdoctoral adviser), Leo and Gordon Baym, as well as with the many bright postdocs who were at Illinois at that time.

M.W.: You have travelled around the globe. What is the status of education

Continued on page 21

Water Footprint and Virtual Water – Emerging Concepts in Water Management

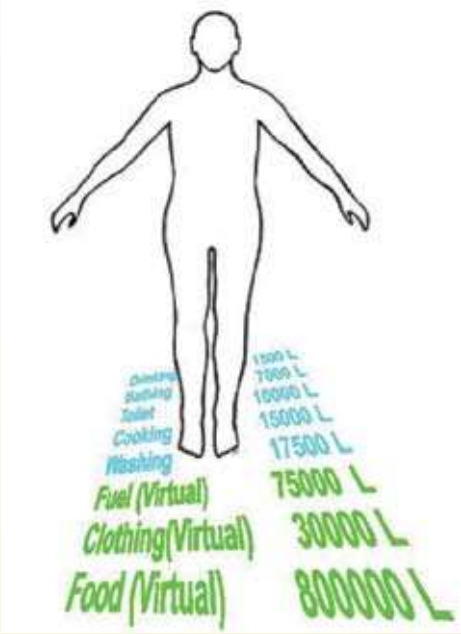
Pradip K Sengupta
E-mail: sengupta_pradip@yahoo.com

During the last few decades water has become the most talked about subject and has been termed as the most precious as well as abused natural resource. As days pass water is becoming the cause of conflict everywhere. It is probable that today's food production and environmental trends, if contained, will lead to crises in many parts of the world. Only if we act to improve water use in every sector we may be able to meet the acute freshwater challenge over the coming 50 years.

Blue water and green water

In recent years, several issues of global changes have given rise to a number of concepts of sustainable use and management of water. Water footprint is a new concept in the field of water management. Generally, consumption of water is measured in terms of water harvested from natural sources and consumed and utilised in various ways. We generally consider the consumption or utilisation of water that is visible and practically measurable. In those terms an urban individual generally utilise about 150 litres of water per day. A rural family consumes much less water. This use encompasses all uses, including drinking, bathing, washing, gardening, etc. We do not take into account of the water that is consumed during the production of any goods or the production of crops in the fields. Terrestrial crops generally do not consume water from the visible sources of water like rivers lakes or groundwater unless the fields are irrigated. They solely depend on soil water, which is not accessible by the animals or humankind as such. So under the new concept of water footprint, water is termed 'blue water' and 'green water' depending on the source. Blue water is available in all visible sources of water like rivers, lakes, ponds and groundwater. But the water that resides in the pore spaces in the soil is called green water. Regarding human consumption of water, we generally consider three major areas – domestic, agricultural and industrial. But these uses are all visible uses that we can directly measure. The consumptive uses of water and its loss from soil to the atmosphere through the process of evapo-transpiration seldom come to our mind.

When rain drops on earth it is divided into two components, the blue water and the green water. The global ratio of blue vs green water is 35:65. But it varies from country to country. In Ghana, for example, the ratio of blue vs. green water is 2.5:97.5 whereas in India the ratio is 35:65. It is



generally assumed that blue water is the runoff water and will flow into the sea or accumulate in water bodies or aquifers. We lift water from these sources, consume a part of it, add to green water through irrigation and also contaminate a part of it. The water we contaminate by the process of washing, cleaning, etc., is called grey water.

Virtual water

The water consumed by the plants is not measurable directly. But It has been possible experimentally to estimate the amount of water consumed by each type of plant or the amount of water required to grow unit mass of plant biomass or crop. Because the process of photosynthesis requires so much water to be transpired in order for CO_2 to be taken in, agriculture accounts for much more virtual water than the industrial processes. The consumptive relation between carbon intake and release of water vapour through the stomata of a plant is extremely asymmetrical. It depends on the how many moles of H_2O are required to fix one mole of CO_2 of a particular plant. As a result most cultivated plants need 900–1,200 moles, and some up to 4,000 moles, of H_2O to fix 1 mole of CO_2.

Thus another concept is developed which is called virtual water. The concept of virtual water had initially been introduced by John Anthony Allan of the School of Oriental and African Studies of the University of London in the early 1990s while studying the water scarcity problems in West Asia. Virtual water is the amount of water required to grow a product. The product may be an agricultural product or an industrial one. Agricultural products like rice, wheat, vegetables require a huge amount of water to grow. For example, virtual water content of rice, wheat and potato are 2,850, 1,400 and 1,000 litres/kg respectively.

Non-vegetable food stuff require a higher quantity of water for its production. A recent study has revealed that in North America the most efficient broiler feed system consumes 2.2 units of feed to produce one unit of broiler mass, out of which only 55% is edible. Hence 4 kg of feed is required to produce 1 kg of edible meat. This amount is much higher in other meats like beef and pork. 1 kg of boneless pork requires 10 kg of feed (corn equivalent). The feed is a combination of soybean (for protein) and corn (for carbohydrate). The water requirement for producing 1 kg of corn and soybean is 500 litres and 1,900 litres respectively. Hence the virtual water content of 1 kg boneless pork comes to be at least 15,000 litres!

The concept of virtual water should not be confused with the actual water content of the biomass or food grain. Food grains are harvested when the moisture content of the crop is at its minimum, viz., 20 to 25%. This moisture content is further made to drop below 14% by drying when it is marketed. So 1 kg of wheat contains only 110 g of actual water when it is marketed.

We may also take virtual water content of products into consideration. The reader

may now be interested in knowing the virtual water contents of the different products or uses in each case or event. It has been calculated that one cup of coffee requires 140 litres of water taking into consideration all aspects of cultivation, processing, and its preparation for the table. Similarly the virtual water content of a T-shirt is 2,000 litres. In this way every product or usage can be expressed in terms of virtual water.

Virtual water trade

Some countries of the world are considered as water-scarce because they do not have adequate water to meet their current and projected water needs, while some other countries are water-rich. Water-rich countries have more water compared to their demands. Further, in big countries there are regions of surplus or deficient water availability. If one country exports a water-intensive product to another country, it exports water in virtual form. In this way some countries support other countries in their water needs. Trade of real water between water-rich and water-poor regions is generally impossible due to the large distances and associated costs, but trade in water-intensive products (virtual water trade) is realistic. It is not wise to produce water intensive products in a water scarce country. They can import it from other countries and keep their domestic water resource for other uses like sanitation, environment and navigation. Moreover there are enough possibilities of a water-intensive country to earn foreign exchange and profit from their water abundance.

Within India there is virtual water flow from state to state. Even the water-scarce states like Punjab and Haryana export virtual water to water-rich states in the east. The eastern states are saving water through import of wheat and rice from other states.

Water footprint

By definition, water footprint is the consumption based assessment of water utilised by an individual, community, product, industry, state, or a country. Any geographical entity can have its own water footprint. Water footprint of an individual or a community is estimated by multiplying all goods and services consumed by their respective virtual-water content.

Finally, water footprint is an indicator of human appreciation of natural capital. Its common denominator is use of freshwater resources.

Calculating a Water Footprint (WF)

For calculating water footprint of an individual, each commodity used by the individual and the virtual water content of those commodities are taken into account and is added to the real blue water used by the individual. The WF of the community is achieved through the accumulation of the data of individuals. If we try to calculate the WF of a household we should take into account the green water footprint by calculating the food consumed and other commodities used in the family and its virtual water content plus the visible water used for drinking, cooking, washing, toilet, gardening, etc. The waste water produced from the household will come into the account of gray water footprint. The unit of water footprint of an individual is cubic metre per capita per year (m^3/cap/year). One can calculate his/ her own water footprint at this website: http://www.waterfootprint.org/?page=cal/WaterFootprintCalculator

Table: Water footprint of some selected nations

Sl No	Country	National (Gm^3/year)	Per capita (m^3/cap/year)
1	Australia	26.56	1,393
2	Bangladesh	116.49	896
3	Brazil	233.59	1,381
4	Canada	62.8	2,049
5	China	883	702
6	Egypt	69.5	1,097
7	France	110.19	1,875
8	Germany	126.95	1,545
9	India	987.38	980
10	Indonesia	269.96	1,317
11	Italy	134.59	2,332
12	Japan	146.09	1,153
13	Jordan	6.27	1,303
14	Mexico	140.16	1,441
15	Netherlands	19.4	1,223
16	Pakistan	166.22	1,218
17	Russia	270.98	1,858
18	South Africa	39.47	931
19	Thailand	134.46	2,223
20	United Kingdom	73.07	1,245
21	USA	636.01	2,483
	Global (Total/ average)	7,452	1,243

Source: Chapagain, A.K., Hoekstra, A.Y. 'Water footprints of nations, Volume 1, 2: Appendices', Value of Water Research Series No. 16, UNESCO-IHE

Calculating a nation's water footprint

Generally, a country does not entirely depend on its own virtual water resources nor is all of its virtual water production entirely consumed within the country. Therefore a nation's water footprint has two components, the internal and the external water footprint. The internal water footprint of a nation is the sum total of the agriculture water use, domestic water use, and industrial water use minus the virtual water export in the form of products produced in the country.

The products imported to a country accounts for the external water footprint (EWFP) of the country. It is defined as the annual volume of water resources used in other countries to produce goods and services consumed by the inhabitants of the country concerned. It is also equal to the virtual water import into the country *minus* the volume of virtual water exported to other countries as a result of re-export of imported products.

Virtual Water Import (VWI) – Virtual Water Export (VWE) = External Water Footprint (EWFP)

So, the total water footprint of a country = internal water footprint + external water footprint.

[The unit of water footprint of a nation is Giga cubic metre per year (Gm^3/yr)]

Water footprint varies from country to country. In a country where the individual (per capita) water footprint is low, the national WF may be very large if the population of the country is large. The global water footprint is 7,450 Gm^3/yr, which is 1,240 $m^3/cap/yr$ on average. The national and average per capita water footprints of some nations are shown in the table below.

Conclusion

The concept of water footprint and virtual water is new. Virtual water deals with the water required for production of a commodity or a service. It is the product-based estimation of water consumption. Water footprint is the consumption-based estimation of water use of an individual, community or country. Virtual water of the same product may vary from one country to other depending on both climate and technology.

Water footprint depends on the lifestyle, food and consumption pattern. By exporting and importing virtual water in the form of products a country can reduce or increase its water footprint. Water footprint of a locality may change if the land use pattern is changed. If an agricultural land is converted into an industrial land or an urban agglomeration the water footprint will change to a great extent. We can appropriately judge whether the land use change would have any adverse effect or not if we calculate the present and future water footprint.

There are several ways postulated by experts to reduce water footprint of a nation. The first is by adopting production techniques that require less water per unit of product. Water productivity in agriculture can be improved for instance by applying advanced techniques of rainwater harvesting and supplementary irrigation.

A second way of reducing water footprints is to shift to consumptions patterns that require less water; for instance, by reducing meat consumption as well as fuel consumption. Water footprint can be reduced if bicycles are used for short-distance travel instead of a car. It has also been observed that meat consumption has an increasing trend worldwide. Consumption pattern may be revised or regulated by appropriately pricing and building awareness.

A third method that can be used is to shift production from areas with low water-productivity to areas with high water-productivity, thus increasing global water use efficiency. For instance, Jordan has successfully externalised its water footprint by importing wheat and rice products from the USA, which has higher water productivity than Jordan.

Water footprint study in India is now at an initial state. Most of the studies in India or on India have been done in mega level covering the whole nation or certain states. Estimates of local area water footprint or virtual water flow from crop land to the consumers have not yet been used for local level planning or development. One or two beverage companies and petrochemical companies are starting to introduce virtual water assessment of their products. In any state of India assessment of water footprint of any land area (watershed, village, forest land, etc.) can be a potential decision support tool before converting a land from agriculture or forest to industries. Such assessment may lead to a prospective planning and also work as an aid to reduce conflicts on water.

References:

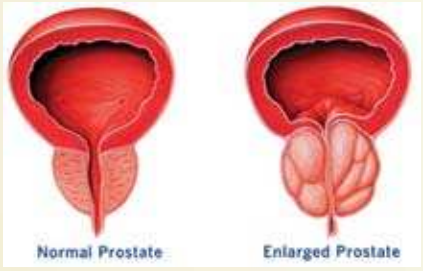
1. Vijay Kumar and Sharad K. Jain (2007). Status of virtual water trade from India, *Current Science*, Vol. 93, No. 8, 25
2. Hoekstra, A.Y. (ed.) (2003). Virtual water trade: Proceedings of the international expert meeting on virtual water trade, Value of Water Research Series No. 12, UNESCO-IHE
3. Chapagain, A.K., Hoekstra, A.Y. (2004). 'Water footprints of nations, Volume 1: Main Report', Value of Water Research Series No. 16, UNESCO-IHE
4. Chapagain, A.K., Hoekstra, A.Y. (2004). 'Water footprints of nations, Volume 2: Appendices', Value of Water Research Series No. 16, UNESCO-IHE
5. Chapagain, A.K., Hoekstra, A.Y., Savenije, H.H.G., Gautam, R., 2006b. The water footprint of cotton consumption: An assessment of the impact of worldwide consumption of cotton products on the water resources in the cotton producing countries. *Ecological Economics* 60 (1), 186–203.
6. Hoekstra, A.Y., Chapagain, A.K., 2007a. Water footprints of nations: water use by people as a function of their consumption pattern. *Water Resources Management* 21 (1), 35–48.
7. Vaclav Smil, (2008), Water News: Bad, Good and Virtual, Rational thinking about water may be key to ensuring a clean, plentiful supply, *American Scientist*, Volume 96, Sigma Xi, The Scientific Research Society.

Benign Prostate Enlargement
Weighing the Treatment Options

Dr Yatish Agarwal
e-mail: dryatish@yahoo.com

It was one of the deadliest and heaviest feelings of my life to feel that I was no longer a boy. From that moment I began to grow old in my own esteem–and in my esteem age is not estimable.
—Lord Byron, Byron's Letters and Journals,Vol. 9

Like grey hair and bald pates, prostate gland enlargement is a common ageing change which occurs in men as they grow older. Doctors often refer to it as benign prostatic hyperplasia (BPH) or benign prostatic hypertrophy, and that's simply their way of saying it's not cancer. However, if you are careless about it and leave it untended, anenlarged prostate can block the flow of urine and produce bothersome bladder and kidney problems.



Several treatments work wellfor prostate gland enlargement. In deciding what makes the best option, your doctor will consider your individualsymptoms,the size of your prostate, the other health problems you may have, and your own preferences. Currently, thefirst lineof treatment revolves around lifestyle changes andmedications. Some men may, however, need surgery. These are those few, who do not do well with medication.

The treatment drill begins with tests and diagnosis, which aimat establishing a definitive diagnosis and quantifying the extent of problem.

Tests and Diagnosis

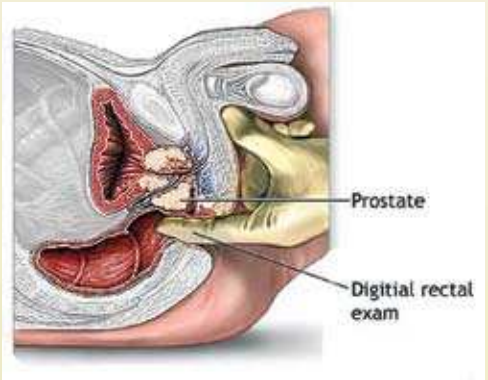
You are likely to first notice the symptoms of prostate gland enlargement yourself, and seek a doctor's help. When prostate enlargement is suspected, it is best to see a surgeon, or preferably, an urologist, a doctor who specialisesin problems of the urinary tract and the male reproductive system. Several tests help the doctor identify the problem. The tests vary from patient to patient, but the following are the most common.

Detailed questions about your symptoms

Your doctor will want to know all about yoursymptoms, what medications you're taking and if you have had an ultrasound examination in the recent. He may also ask you to complete a questionnaire such as the American Urological Association (AUA) Symptom Index for benign prostatic hyperplasia.

Digital rectal examination

This examination is usually the first test done. The doctor inserts a gloved finger into the rectum and feels the part of the prostate next to the rectum. This examination gives the doctor a general idea of the size and condition of the gland.



Prostate-Specific Antigen (PSA) Blood Test

To rule out prostate cancer, your doctor may recommend a PSA blood test. PSA, a protein produced by prostate cells, is frequently present at elevated levels in the blood of men who have prostate cancer.

A PSA test when used in conjunction with a digital rectal examination can help detect prostate cancer in men who are age 50 or older and for monitoring men with prostate cancer after treatment. However, much remains unknown about the interpretation of PSA levels, the test's ability to discriminate cancer from benign prostate conditions, and the best course of action following a finding of elevated PSA.PSA levels can also be elevated due to recent rectal digital examination, rectal ultrasound tests, surgery or infection (prostatitis).

Trans-Rectal Ultrasound

An ultrasound test provides measurements of your prostate and also reveals the particular anatomy of your prostate. With this procedure, an ultrasound probe about the size and shape of a large cigar is inserted into your rectum. Ultrasound waves bouncing off your prostate create an image of your prostate gland.

Post-void residual volume test

This test measures whether you can empty your bladder completely. This is often done by using an ultrasound test to measure urine left in your bladder immediately after you have voided the bladder.

Prostate biopsy

If there is the slightest suspicion of prostate cancer, your doctor may recommend a biopsy test with guidance under rectal ultrasound. In this procedure, a probe inserted in the rectum directs sound waves at the prostate. The echo patterns of the sound waves form an image of the prostate gland on a display screen. To determine whether an abnormal-looking area is indeed a tumour, the doctor can use the probe and the ultrasound images to guide a biopsy needle to the suspected tumour. The needle collects a few pieces of prostate tissue for pathological examination with a microscope.

Urinary flow test

This test measures the strength and amount of the urine flow. You are asked to urinate into a receptacle attached to a special machinethat measures how quickly the urine is flowing. A reduced flow often suggests prostatic enlargement.The results of this test over time help determine if your condition is getting better or worse.