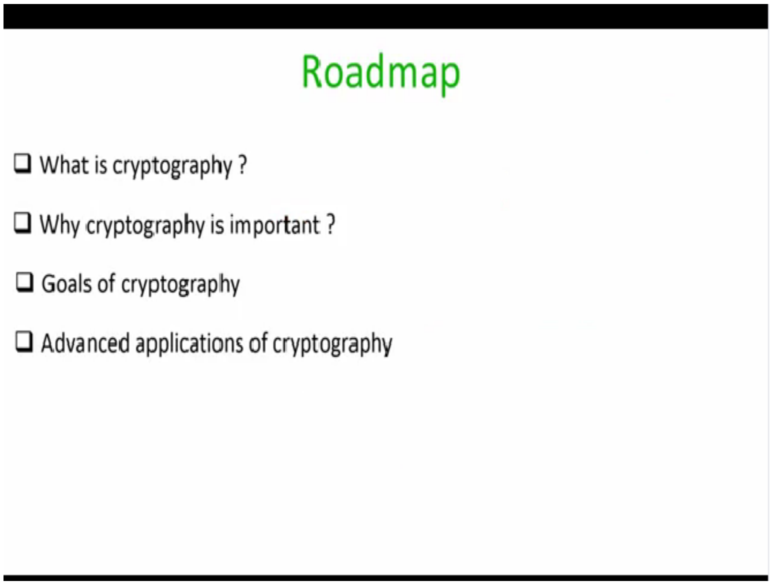
Foundations of Cryptography

Prof. Dr. Ashish Choudhury
(Former) Infosys Foundation Career Development Chair Professor
International Institute of Information Technology-Bengaluru

Lecture-01
Introduction

So, hello everyone, welcome to the first lecture on the foundations of cryptography course.

(Refer Slide Time: 00:34)



Roadmap

- ❑ What is cryptography ?
- ❑ Why cryptography is important ?
- ❑ Goals of cryptography
- ❑ Advanced applications of cryptography

The plan for this lecture is as follows. We will discuss what is cryptography, why cryptography is important, what are the goals of cryptography and we will see some of the advanced applications of cryptography.

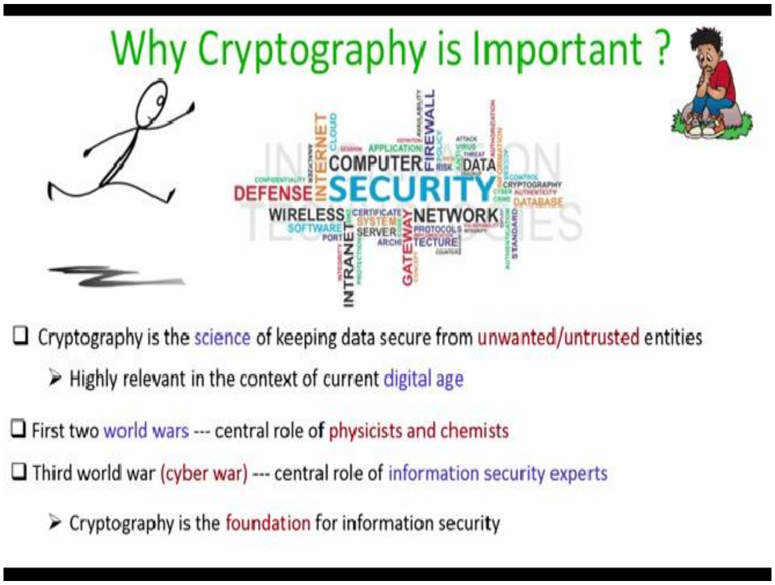
(Refer Slide Time: 00:48)

Importance of Strong Foundation ?

❑ Strong foundation is very important for a long-lasting building

So, since the title of the course is foundations of cryptography, let us first try to understand the importance of strong foundation. So, if you see these 2 buildings or pictures of these 2 buildings you can easily understand that if you want a long lasting building then strong foundation is very important.

(Refer Slide Time: 01:07)



Why Cryptography is Important ?

❑ Cryptography is the science of keeping data secure from unwanted/untrusted entities

➢ Highly relevant in the context of current digital age

❑ First two world wars --- central role of physicists and chemists

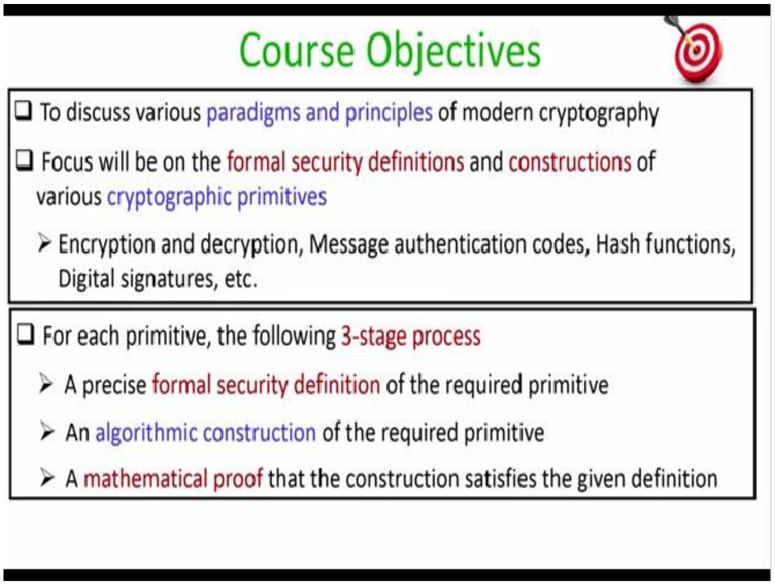
❑ Third world war (cyber war) --- central role of information security experts

➢ Cryptography is the foundation for information security

So why cryptography is important. So security is currently a very big buzzword, everyone is talking about security they want to keep their system secure. So cryptography on a very high level is the science of keeping data secure from unwanted or untrusted entities. And it is highly relevant in the current context of digital age where things are becoming digital slowly and slowly. And as a result, we have large amount of data floating around at various places.

So, if you consider the first 2 world wars, the roles of physicists and chemists was very central. And it is predicted that if at all there is a third world war, then it will be a cyber war, where the role of information security experts will be very crucial. So cryptography is the foundations for information security. And if you want to become a good information security expert, then it is very important to have strong foundations for cryptography.

(Refer Slide Time: 02:07)



Course Objectives

❑ To discuss various paradigms and principles of modern cryptography

❑ Focus will be on the formal security definitions and constructions of various cryptographic primitives

➢ Encryption and decryption, Message authentication codes, Hash functions, Digital signatures, etc.

❑ For each primitive, the following 3-stage process

➢ A precise formal security definition of the required primitive

➢ An algorithmic construction of the required primitive

➢ A mathematical proof that the construction satisfies the given definition

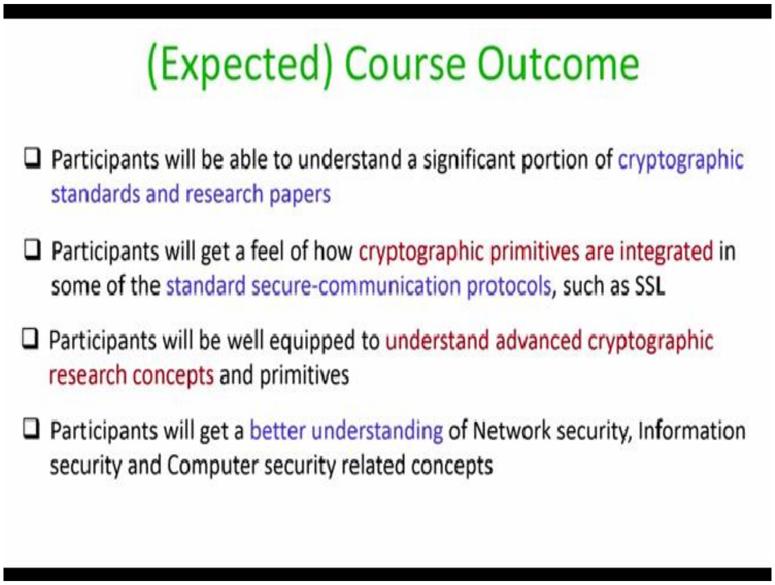
So, the objectives of the course are as follows. We will discuss the various paradigms and principles of modern cryptography and the focus will be on formal security definitions and constructions of various cryptographic primitives. So, some of the cryptographic primitives which we will discuss in this course are encryption and decryption, message authentication codes, hash functions, digital signatures, etc.

Now, for each of these cryptography primitives, we will follow the following 3 stage process. In first stage we will give a precise formal security definition of the underlying primitive that we are interested to construct. Once we have the formal security definition, we will proceed to give an algorithmic construction of the required primitive and finally, in stage 3 we will give a rigorous mathematical proof that the algorithmic construction which we have given in stage 2 indeed satisfies the formal definition that we gave in stage 1.

So you can compare this 3 stage process with the following example. If you want to build a house, what you will first do is you will come up with a rough architecture of the house, and you will have the map of the house, which you give to your engineer. So that is a stage 1. Once the map is ready, during stage 2 the engineer will involve some workers and some other helpers using whom he will come up with the building. That is algorithmic construction.

And in stage 3 once the building is ready, you will indeed verify that the construction which the engineer has come up with indeed satisfies the architecture which you actually specified during stage 1. So that is a 3 stage rigorous process which we are going to follow in this course for each of the cryptographic primitives that we will discuss.

(Refer Slide Time: 03:50)



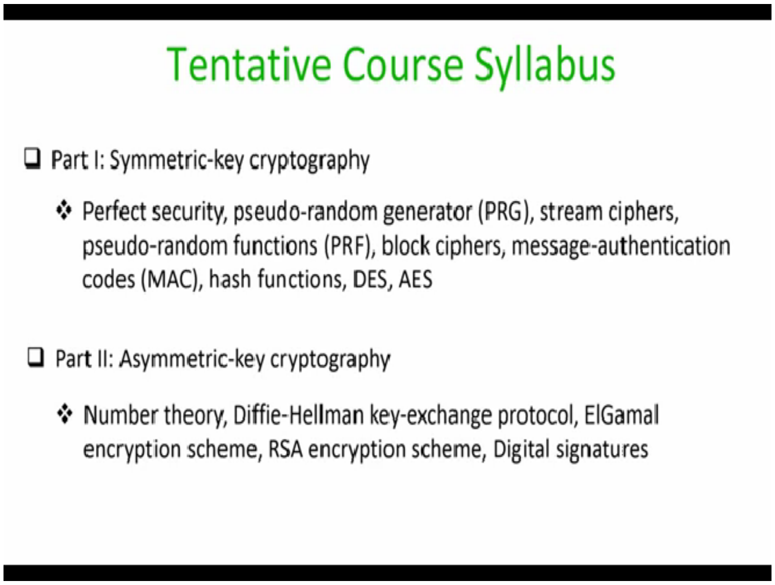
(Expected) Course Outcome

- □ Participants will be able to understand a significant portion of cryptographic standards and research papers
- □ Participants will get a feel of how cryptographic primitives are integrated in some of the standard secure-communication protocols, such as SSL
- □ Participants will be well equipped to understand advanced cryptographic research concepts and primitives
- □ Participants will get a better understanding of Network security, Information security and Computer security related concepts

The expected course outcome are as follows. We expect at the end of the course participants will be able to understand a significant point of cryptography standard and research papers, we hope that participants will get a feel of how the various cryptographic primitives that we will discuss in this course are integrated in some standard secure communication protocols such as SSL. We hope that participants will be well equipped to understand advanced cryptography research concepts and primitives.

And in general participants will get a better understanding of concepts related to network security, information security and computer security in general.

(Refer Slide Time: 04:32)



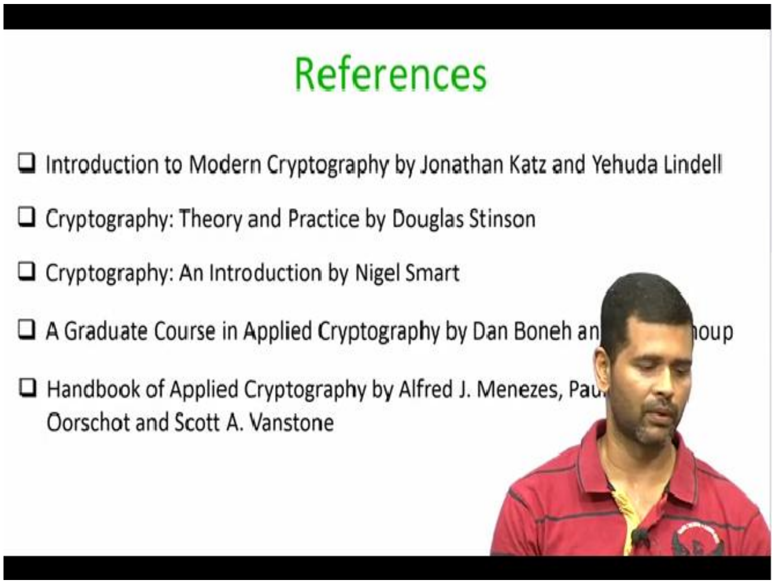
Tentative Course Syllabus

- ❑ Part I: Symmetric-key cryptography
  - ❖ Perfect security, pseudo-random generator (PRG), stream ciphers, pseudo-random functions (PRF), block ciphers, message-authentication codes (MAC), hash functions, DES, AES
- ❑ Part II: Asymmetric-key cryptography
  - ❖ Number theory, Diffie-Hellman key-exchange protocol, ElGamal encryption scheme, RSA encryption scheme, Digital signatures

So, as far as the course syllabus is concerned, the tentative syllabus is as follows. Roughly the course is divided into 2 parts. The first part is going to discuss symmetric key cryptography, where we are going to discuss perfect security, pseudo random generators, stream ciphers, pseudo random functions, block ciphers, message authentication codes, hash functions, and some of the practical constructions of block ciphers like the DES and AES.

In part 2 we will be discussing about asymmetric cryptography and some of the topics which we will be covering in part 2 are number theory, Diffie-Hellman key exchange protocol, ElGamal encryption scheme, RSA encryption scheme and digital signatures.

(Refer Slide Time: 05:16)



References

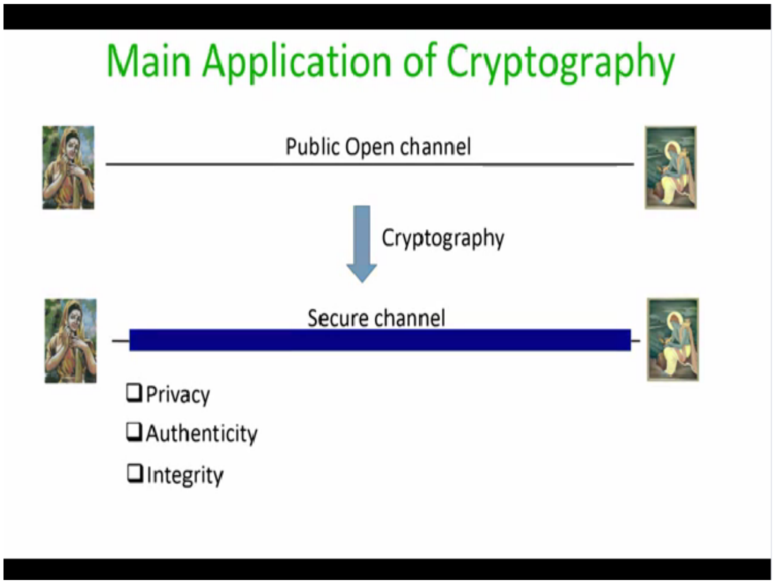
- □ Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell
- □ Cryptography: Theory and Practice by Douglas Stinson
- □ Cryptography: An Introduction by Nigel Smart
- □ A Graduate Course in Applied Cryptography by Dan Boneh an houp
- □ Handbook of Applied Cryptography by Alfred J. Menezes, Pau
  Oorschot and Scott A. Vanstone

We will be following the following references in this course. So the course will be mostly based on the book titled Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell. And this is really one of the standard textbook which is widely followed. And I recommend everyone who is interested to learn cryptography and foundations of cryptography to purchase a personal copy of this book. You can also follow the book Cryptography: Theory and Practice by Douglas Stinson.

You can also refer to the book by Professor Nigel Smart titled Cryptography: An Introduction. The first version of this book in fact is available free to download from the author's homepage and you can see the following interesting book: A Graduate Course in Applied Cryptography by Dan Boneh and Victor Shoup, again, the draft of this book is available free to download. And you can also refer to the Handbook of Applied Cryptography by Menezes et al, which again is available free to download.

So, these are some of the important references, which we will be following in this course. Of course, if you do the Google search, you can come up with plenty of other important references, which you can follow for the various topics which we are going to follow in this course.

(Refer Slide Time: 06:30)



Main Application of Cryptography

Public Open channel

Cryptography

Secure channel

- ❑ Privacy
- ❑ Authenticity
- ❑ Integrity

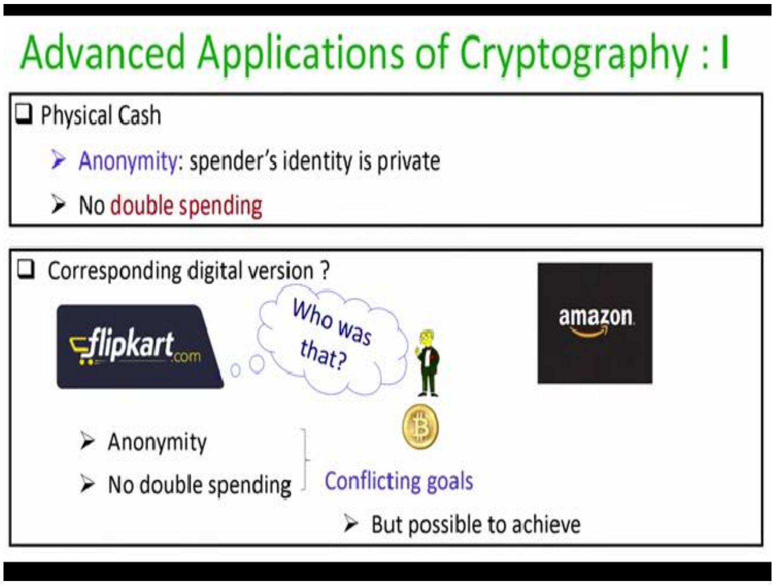
Coming back to the question of what is the main application of cryptography. So, the central problem that is addressed by cryptography is that of secure communication. And what I mean by secure communication is imagine the following scenario that you have a sender and a receiver who do not know each other who are meeting for the first time over the internet. They do not share any kind of pre-shared information. And they are connected by a public open channel. So, the main goal of the cryptography is to somehow convert this public open channel connecting the sender and the receiver into some kind of virtual secure channel through which sender and receiver can do secure communication. And the 3 properties of the secure communication are as follows. The first property is the privacy, which ensures that anything which is communicated between the sender and the receiver over this virtual secure channel will be known only to the sender and the receiver.

The next property of the secure communication is the authenticity which ensures that any message or any packet which comes to the sender over this channel from the receiver, is confirmed that it is indeed originating from the receiver and there is no third party who has introduced those packets on the behalf of the receiver and forwarded it to the sender and the same guarantee will be given at the receiver’s end as well.

And the third property of the secure channel will be integrity property, which will ensure to the sender and the receiver that no one has tampered upon the contents of the packets which have been communicated over the channel. So on a very high level the cryptographic primitives that we will be discussing in this course will give you the effect of converting this public open channel into some kind of virtual secure channel.

And no third party will be able to identify what exactly is flowing around through this secure channel. That is the main application of cryptography.

(Refer Slide Time: 08:30)



Advanced Applications of Cryptography : I

❑ Physical Cash
- ➢ Anonymity: spender's identity is private
- ➢ No double spending

❑ Corresponding digital version ?
- ➢ Anonymity
- ➢ No double spending

Conflicting goals
- ➢ But possible to achieve

flipkart.com
Who was that?
amazon

And which we are going to rigorously discuss in this course. But what I would like to go through in the next few slides is some of the advanced applications of cryptography. The main idea is that I want to give you a feeling of that how cryptography can be used to solve varieties of other kinds of real world problems apart from the problem of secure communication. So the first advanced application that I would like to discuss upon is that of cryptocurrency.

So before going into cryptocurrency, let us understand the 2 important properties that are satisfied by your physical cash or fiat currency. So the 2 properties are it prevents double spending. That means it is impossible for you to create xerox copies of a physical note and spend it at multiple locations. So that is the double spending problem and physical cash ensures that indeed double spending is not possible.

And the second property of the physical cash is anonymity. That means if I am using a physical currency and spending it for some transaction, now my identity will be preserved. But because no one will be able to track down my identity, who is spending that currency and so on. So that is the anonymity property. So the question is can we have a corresponding digital version of the physical cash.

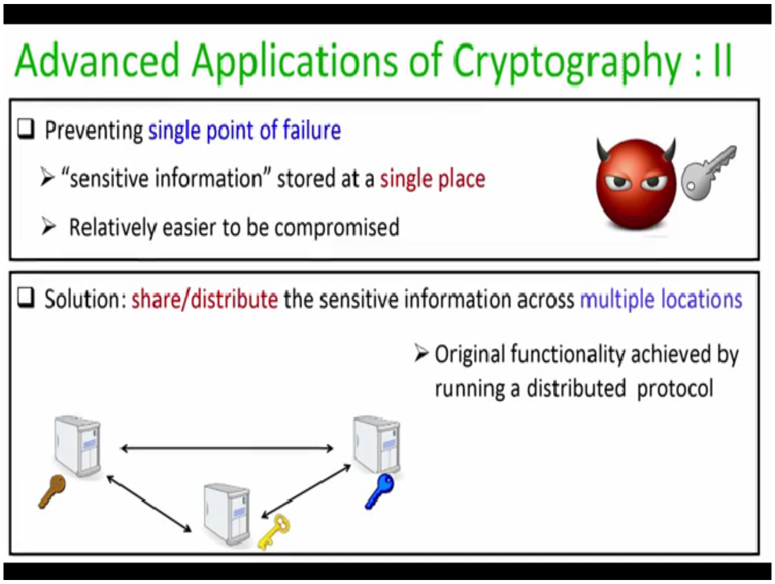
And when I say the digital version, what I mean is that now a bit string will act as a currency and using this bit string, I should be able to do transactions at any merchant site. And when I do a transaction at any merchant site, and try to spend this binary string as a currency, the anonymity property should be achieved that means the merchant should not be able to identify the owner of this so called binary string or digital currency.

And the second property that I would like to achieve from the corresponding digital version of the currency is no double spending, that means it should be difficult for me to create multiple copies of this binary string and spend those copies of the binary string simultaneously at multiple locations. Interestingly, I would like to achieve both these 2 properties in the absence of any centralized agency.

That means I want the whole system to work even in the absence of any kind of centralized agency. And as you can see, if there is no centralized agency who is actually monitoring who is spending which binary string at which location, it looks like that anonymity problem and a no-double spending problem, are like two conflicting goals. But if you see the recent cryptocurrency like bitcoin, it is possible to achieve both these two requirements simultaneously.

So that is like an advanced application of cryptography where the goal is something much, much more challenging than what is required from the problem of secure communication.

(Refer Slide Time: 11:18)



Advanced Applications of Cryptography : II

❑ Preventing single point of failure

➢ "sensitive information" stored at a single place

➢ Relatively easier to be compromised

❑ Solution: share/distribute the sensitive information across multiple locations

➢ Original functionality achieved by running a distributed protocol

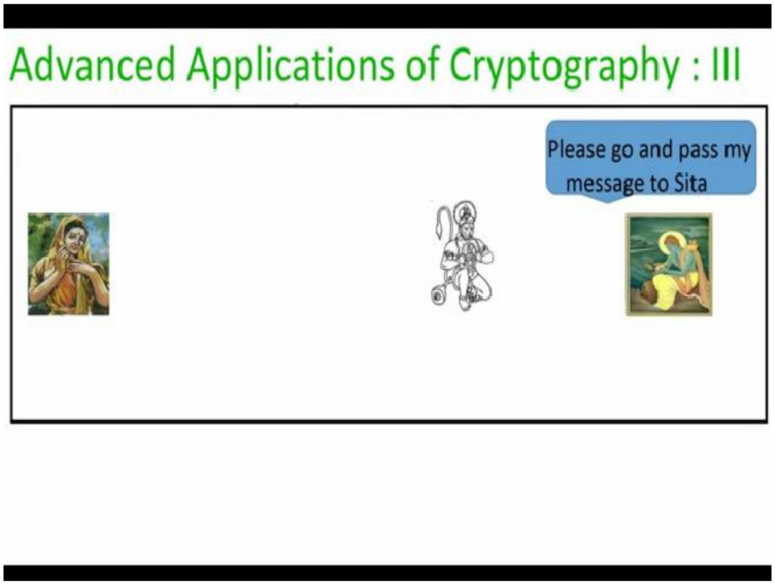
Let us see the second advanced application of cryptography. And this is something what we call as preventing the single point of failure. So it so happens that in many real world applications, sensitive information is stored at a single place. And by sensitive information, I mean, say example, your encryption key or your signature key. So if the sensitive information or the credential is stored at a single place then it becomes relatively easier for an adversary to compromise that single place where the sensitive information is stored, and as a result the entire application will be compromised. So a solution to prevent a single point of failure will be as follows. Instead of storing the sensitive information at a single place, what we can do is we can create shares of that sensitive information and distribute those shares and store it at multiple locations.

And then erase the initial sensitive information. And whatever original function that was supposed to be carried out by the sensitive information will be now carried out by running a distributed protocol among the various servers where the shares of the original sensitive information is stored. Notice that in this entire process, nowhere we reconstruct back the original sensitive information.

The sensitive information is still shared or distributed among the multiple locations and we run a distributed protocol without actually reconstructing back the sensitive information. The advantage of sharing or distributing the sensitive information across multiple location is that it will be now difficult for an adversary to simultaneously compromise all the servers where the shares of the original sensitive information is stored. And as a result, you get more robustness and more fault tolerance.

So this is again a very nice advanced application of cryptography, which is based on a wonderful primitive called as secret sharing. On a very high level, a secret sharing protocol allows you to create shares of a secret and distribute to the shareholders, such that the original secret can be reconstructed back only if certain threshold number of shareholders come together and combine their shares. But if you have a number of shareholders, which is less than that per specified threshold, it will be impossible to reconstruct back the original secret.

(Refer Slide Time: 13:41)

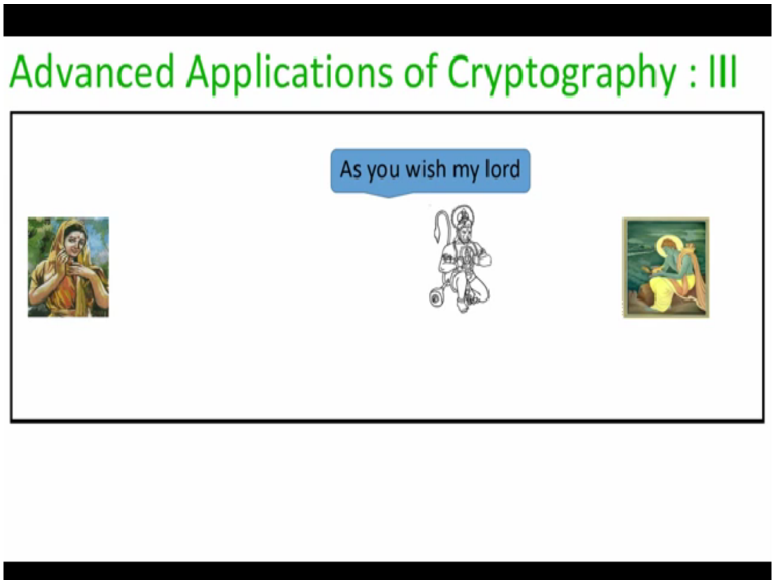


Advanced Applications of Cryptography : III

Let us see another fascinating advanced application of cryptography. And to motivate this application, let me quote an example the wonderful Sundar Kaand from our epic Ramayana, so the people who are familiar with Sundar Kaand will easily under this. So, in the Sundar Kaand the scenario is the following mother Sita is been kidnapped by Ravana and she is in Sri Lanka and Ram is in India.

And since Ram is missing Sita he is very sad. So, he says to his messenger namely Hanuman, that oh Hanuman, please go to Lanka and pass my message to Sita that I am missing her.

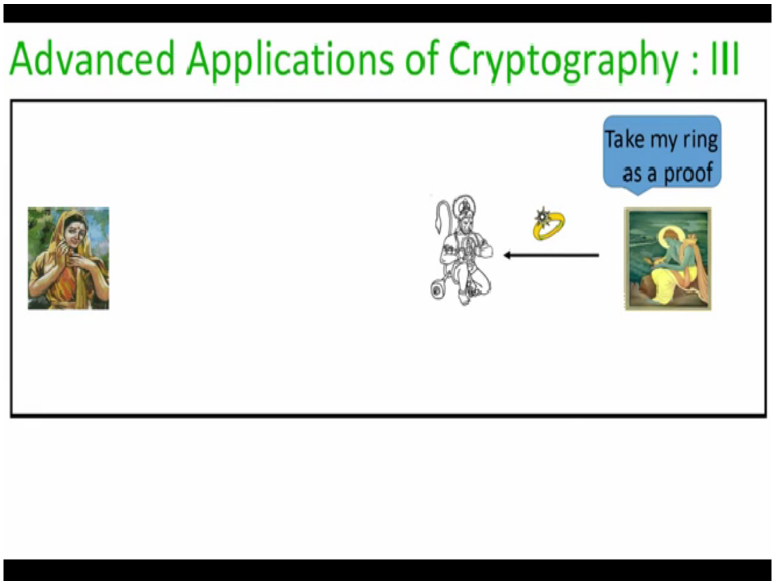
(Refer Slide Time: 14:21)



Advanced Applications of Cryptography : III

And the messenger says, okay lord, as whatever you wish I will follow your instruction.

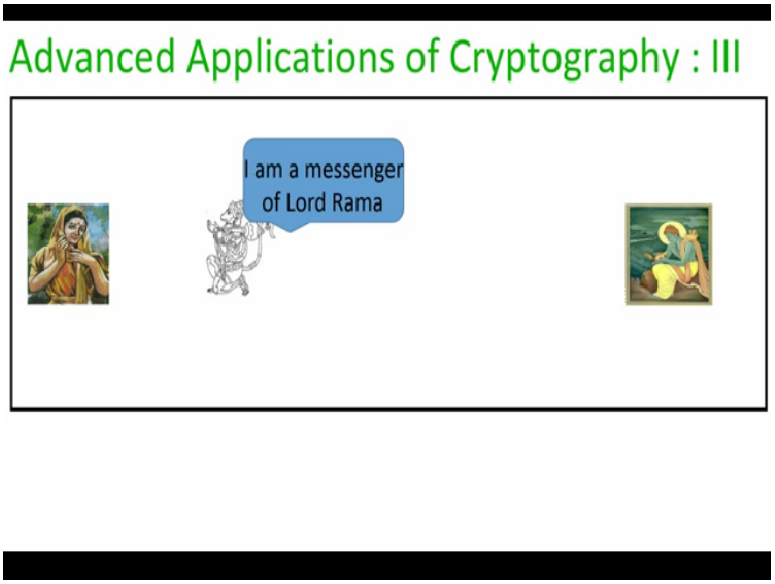
(Refer Slide Time: 14:27)



Advanced Applications of Cryptography : III

But then Ram says that since you are going to meet Sita for the first time, Sita may not be able to identify you. So, what you do is the following you take this ring as a proof that indeed you are my messenger. And if Sita asks you for a proof, you can give this you can show this ring and she will be able to identify you. So, the messenger takes the proof and he starts the wonderful journey comes to Sri Lanka and he lands in Ashoka Vatika and starts the conversation with mother Sita, where he says that oh mother I am the messenger of lord Ram.

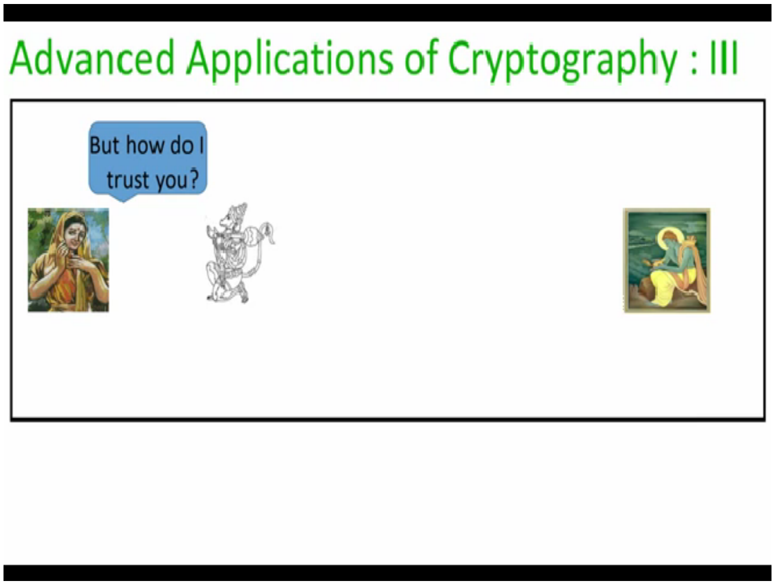
(Refer Slide Time: 15:00)



Advanced Applications of Cryptography : III

But Sita is very scared.

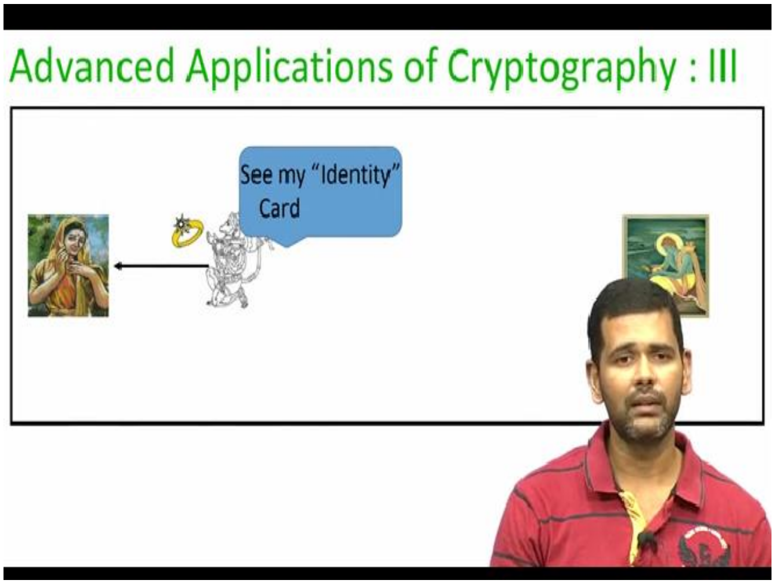
(Refer Slide Time: 15:04)



Advanced Applications of Cryptography : III

She is already harassed by the people of Ravana. So she is unable to trust Hanuman. She says how can I trust you.

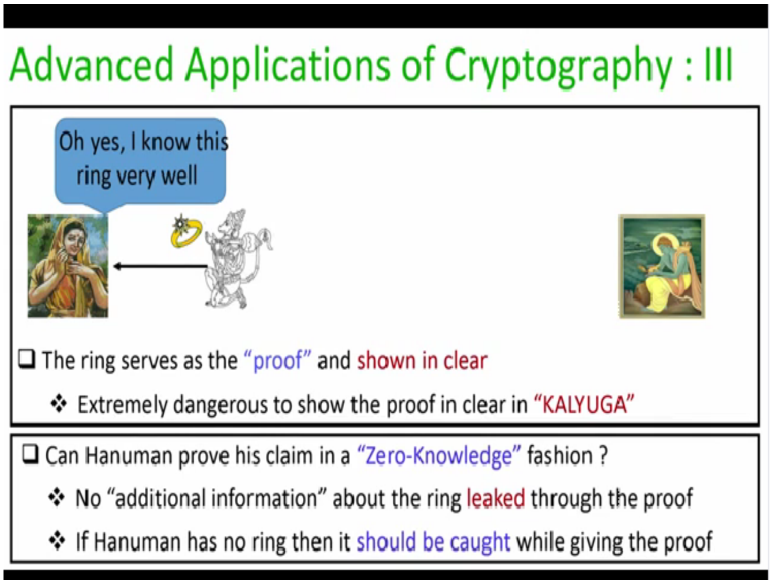
(Refer Slide Time: 15:13)



Advanced Applications of Cryptography : III

So here Hanuman shows the proof namely the ring that Ram gave to Hanuman, and as soon as the ring is shown to Sita.

(Refer Slide Time: 15:20)



Advanced Applications of Cryptography : III

❑ The ring serves as the "proof" and shown in clear

- ❖ Extremely dangerous to show the proof in clear in "KALYUGA"

❑ Can Hanuman prove his claim in a "Zero-Knowledge" fashion ?

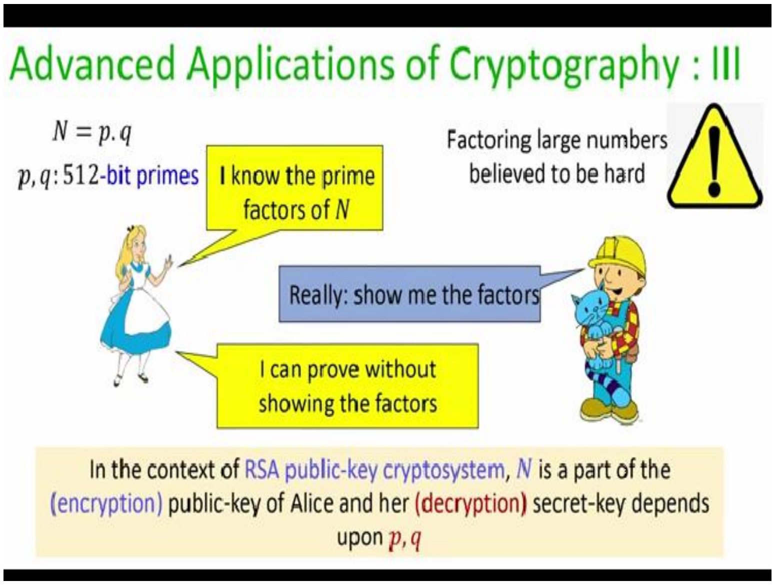
- ❖ No "additional information" about the ring leaked through the proof
- ❖ If Hanuman has no ring then it should be caught while giving the proof

She happily identifies the ring and says, yes, I know this ring very well, and indeed I trust you. So in this example, the ring serves as a proof which is given and shown in clear by the messenger, the messenger is making a statement or a claim that he is indeed the messenger of Ram. And to prove his claim he is actually showing the proof in clear, namely the ring. And that was possible in the age of Sathyuga.

Because people there would indeed used to speak the truth, but showing proof in clear is very dangerous in the current world of Kaliyuga. So, now the question is, is it possible for Hanuman to prove his statement namely, he is the messenger of Ram in a zero knowledge fashion. And what I mean by zero knowledge fashion is, the proof should not reveal anything about the ring. And it should only prove the statement that Hanuman is indeed the messenger of Ram.

That means no additional information about the ring should be leaked through the proof. And more importantly, if Hanuman does not possess the ring, then while giving the proof he should be caught and should be rejected. So a zero knowledge proof system or a zero knowledge protocol ensures approver to prove a statement without revealing anything about the proof.

(Refer Slide Time: 16:39)



Advanced Applications of Cryptography : III

$N = p.q$

p, q: 512-bit primes

I know the prime factors of N

Factoring large numbers believed to be hard

Really: show me the factors

I can prove without showing the factors

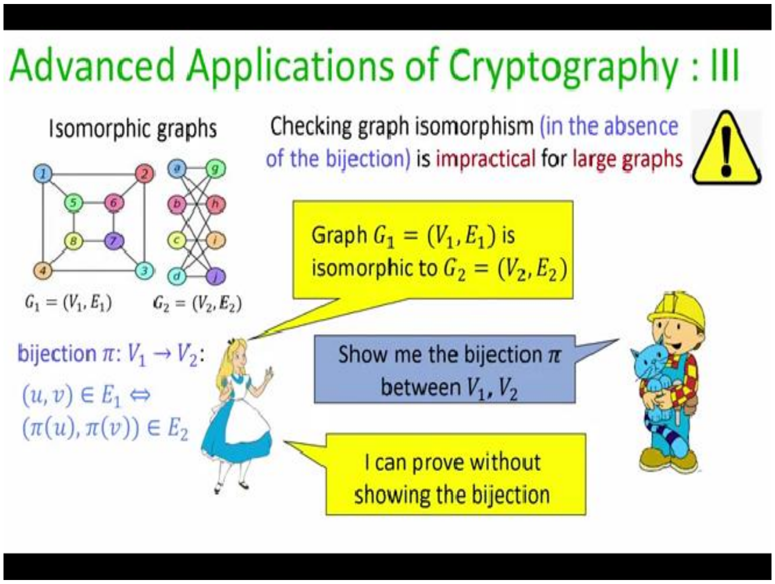
In the context of RSA public-key cryptosystem, N is a part of the (encryption) public-key of Alice and her (decryption) secret-key depends upon p, q

So now let us see an application of zero knowledge proof in the context of computer science namely, in the context of cryptography. So imagine Alice and Bob are 2 entities and say Alice has picked 2 large prime numbers P and Q, which are random prime numbers P and Q of say 512 bits each, and she multiplies the primes P and Q to obtain the number N, and she makes a claim to Bob that hey Bob, I know the prime factors of N.

And Bob says, well, I can check your claim provided you show me the factors of N because indeed if Alice knows the factors, and if she shows the factors P and Q to Bob and Bob can himself multiply P and Q and check whether the product is indeed equal to N or not. So here P and Q are actually the proof, which Alice can show to Bob. But a zero knowledge protocol will allow Alice to convince Bob that indeed she knows P and Q without actually showing P and Q.

So people who are familiar with RSA public cryptosystem, they can relate this example to the RSA cryptosystem because in the context of RSA public key cryptosystem, N is actually the modules and it is part of the encryption key which Alice possess, and it will be publicly available whereas P and Q will be part of a decryption key which will be available only to Alice. Now, you might be wondering that why Bob himself cannot factor out N. Well, it is believed that factoring large numbers is indeed are computationally challenging problem.

(Refer Slide Time: 18:13)



Advanced Applications of Cryptography : III

Isomorphic graphs

Checking graph isomorphism (in the absence of the bijection) is impractical for large graphs

$G_1 = (V_1, E_1)$ $G_2 = (V_2, E_2)$

bijection $\pi: V_1 \rightarrow V_2$:
$(u, v) \in E_1 \Leftrightarrow$
$(\pi(u), \pi(v)) \in E_2$

Graph $G_1 = (V_1, E_1)$ is isomorphic to $G_2 = (V_2, E_2)$

Show me the bijection π between V_1, V_2

I can prove without showing the bijection

Now let us see another related application of zero knowledge protocol. So, here the scenario is the following. So, imagine, Alice has created an isomorphic copy of a graph which she possesses. So, what I mean by isomorphic graphs is the following. If you consider the graphs G_1 and G_2, even though structurally they are drawn in a different manner, property wise they are same, that means they have the same number of vertices. And they have the same number of edges. And more importantly, there exist a bijection, namely a one to one and on to mapping from the vertex set of the first graph to the vertex set of the second graph, such that the following relationship hold, if there is an edge between the node u,v in the first graph then there exists an edge between the mapped vertex u and the mapped vertex v in the second graph and vice versa.

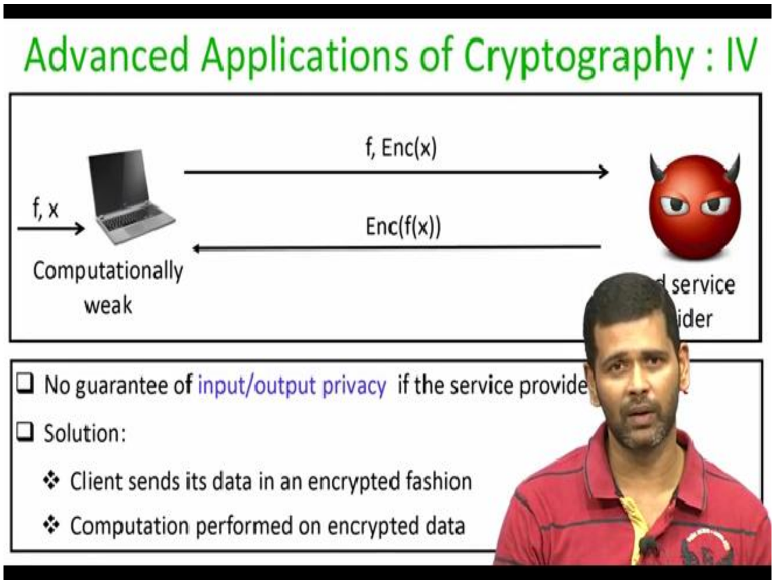
In that sense, these 2 graphs are isomorphic in nature. So imagine Alice started with the graph G_1, and she creates an isomorphic copy of the graph G_1 to obtain the graph G_2. And to obtain the isomorphic graph G_2 what she has to basically do is she has to just take a random permutation of the vertex set of the first graph, and that is the secret information which Alice possesses. And now suppose Alice makes the 2 graphs, G_1 and G_2 public.

And goes to Bob and says, hey Bob, I can prove to you that the graph G_1 and G_2 are isomorphic in nature. Again, people who are familiar with graph isomorphism problem, they will be aware that checking the graph, checking whether 2 graphs are isomorphic or not, in the absence of the bijection is indeed believed to be a computationally difficult problem, if the graphs are of very large magnitude.

So Alice is now interested to prove that the graphs are isomorphic in nature without actually showing the graph isomorphism. So Bob challenges Alice and says, well, if indeed you want to prove that the 2 graphs are isomorphic, show me the isomorphism or the bijection, because if you show me the bijection then I can easily verify whether the 2 graphs G_1 and G_2 are isomorphic in nature.

But using a zero knowledge protocol, Alice can convince Bob that indeed the 2 graphs, G_1 and G_2 are isomorphic. And in the process, Bob will learn no information about the actual bijection, which maps the graph G_1 to the graph G_2. So again, this is a very advanced application of cryptography.

(Refer Slide Time: 20:41)



Advanced Applications of Cryptography : IV

- ❑ No guarantee of input/output privacy if the service provide
- ❑ Solution:
  - ❖ Client sends its data in an encrypted fashion
  - ❖ Computation performed on encrypted data

And the next advanced application of cryptography that I would like to discuss is that of outsourcing computation. So in this problem, the scenario is the following. We have a computationally weak client, and it wants to carry out some kind of computation. So let us abstract out that computation by a function f, and it possesses some data x and it wants to compute the value of the function on the data x.

But since it is a computationally weak processor, it does not have the capability to carry out the computation on its own. So what it does is, it engages the service of a cloud service provider, and it outsources the computation of the function to the cloud service provider by giving him the description of the function as well as the data x. So since the function is available to the cloud service provider, as well as the data is available to the cloud service provider.

A cloud service provider can carry out the computation itself and can send back the result to the computationally weak client. Well, in principle, the solution will work. But the problem here is what if the cloud service provider is a corrupt guy. In this case, there is no guarantee of input output privacy because the client is giving the data in clear to the service provider and as a result, the service provider will be completely aware of the data on which it has carried out the computation.

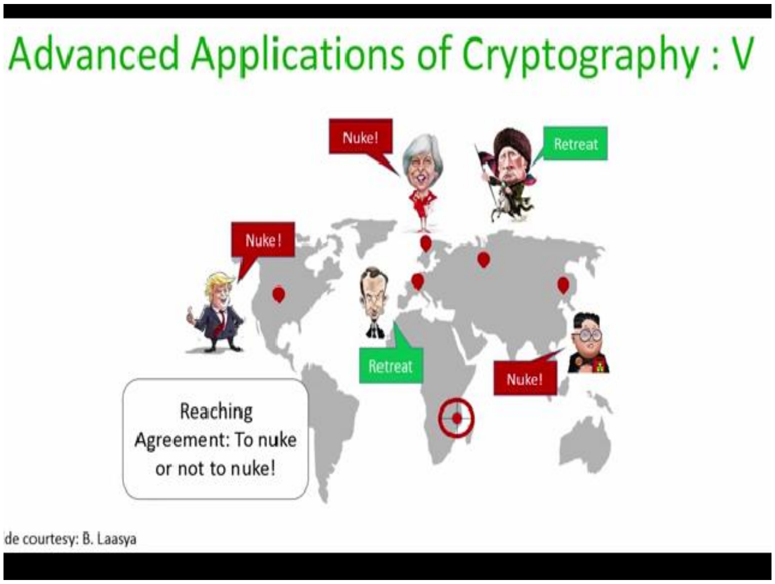
And it will be also aware of the result of the computation. So what if we want to prevent the cloud service provider from knowing the data. The question here is, is it possible for the computationally weak client to not reveal the data and still outsource the computation. So, a potential solution will be that instead of sending the data and clear, it can send an encrypted version of the data and the description of the function.

And instead of carrying out the computation on that clear data, the cloud service provider should be able to carry out the same function on the encrypted data. And it should send back the result of the computation again in an encrypted fashion, which the computationally weak client can decrypt back. So now, you might be wondering, what is the problem with the proposed solution. The problem here is that since the data is now available in an encrypted fashion.

How can a cloud service provider carry out the computation without knowing the data. So till 12 years back this problem was believed to be a very difficult problem because we did not have any form of encryption which can support this proposed solution. That means there was no form of encryption scheme where it was possible to carry out the computation on the encrypted data.

But 12 years back in 2006, history was made where the first candidate proposal for such kind of special encryption scheme which we call as fully homomorphic encryption scheme has been proposed. So on a very high level, a fully homomorphic scheme allows you to carry out computation on the encrypted data without actually knowing the data. So that is again, a very advanced application of cryptography.

(Refer Slide Time: 23:48)



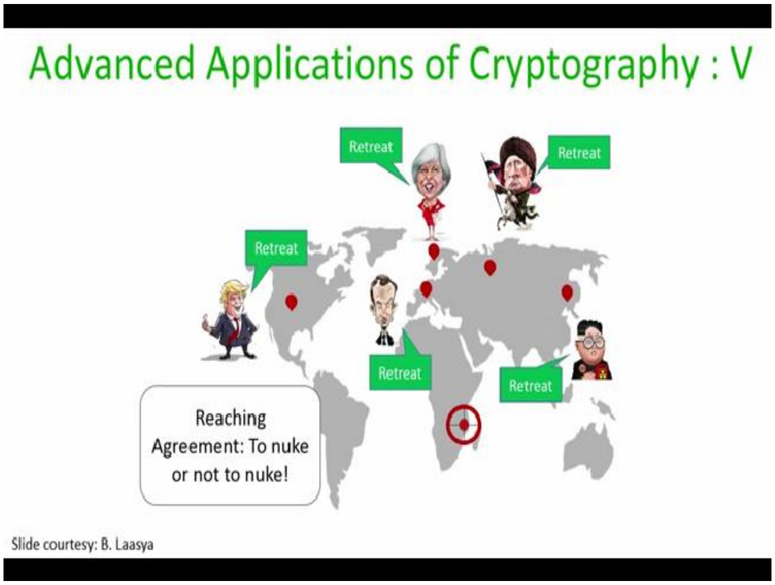
Advanced Applications of Cryptography : V

Reaching Agreement: To nuke or not to nuke!

de courtesy: B. Laasya

The next advanced application of cryptography that I am going to discuss is that about distributed consensus. So imagine the following scenario we have a set of mutually distrusting world leaders. And together they would like to come to a decision whether to attack a particular country or not. That means they would like to run a protocol among each other where they exchanged messages as per the protocol and the end of the protocol, all the leaders should be on the same page.

(Refer Slide Time: 24:16)



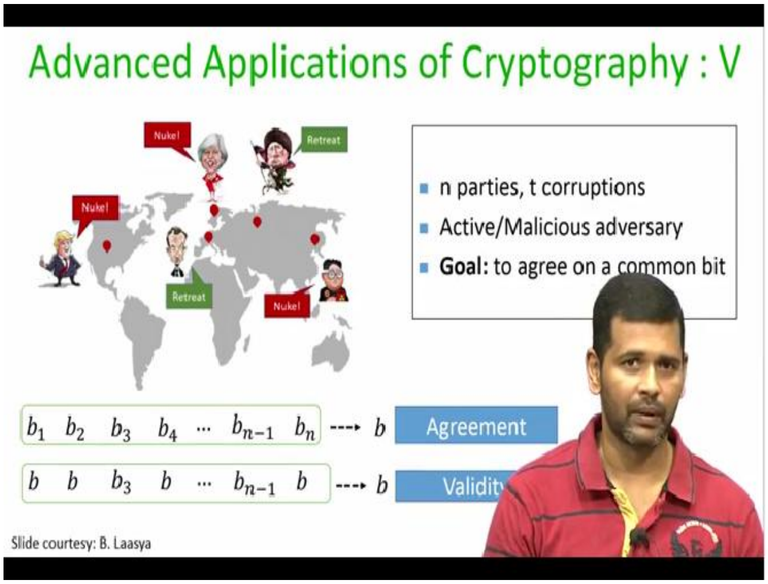
Advanced Applications of Cryptography : V

Reaching Agreement: To nuke or not to nuke!

Slide courtesy: B. Laasya

So the abstraction of this problem is what we call as distributed consensus problem.

(Refer Slide Time: 24:23)



Advanced Applications of Cryptography : V

- n parties, t corruptions
- Active/Malicious adversary
- **Goal:** to agree on a common bit

b_1 b_2 b_3 b_4 ⋯ b_{n-1} b_n ----→ b Agreement

b b b_3 b ⋯ b_{n-1} b ----→ b Validit

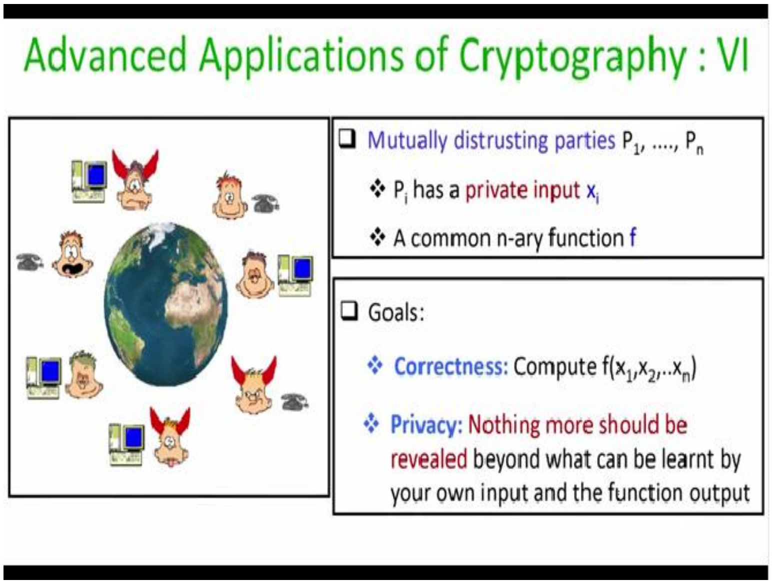
Slide courtesy: B. Laasya

And in the distributed consensus problem, we have a set of n mutually distrusting parties, and t of them could be corrupt. And each of the party has a private bit which could be either 0 or 1. For example, in this specific context. 0 means not to nuke attack the country 1 means to attack the country. So each entity has a private input. And the goal is to run a protocol among these entities so that at the end of the protocol, all the good entities should be on the same page.

That means they should obtain a common bit as the output that is the agreement property I require from the protocol. And the second property I require from the protocol is that if at the beginning itself, all the good entities were on the same page. That means they all had the same common input say b, then the output of the algorithm should be b only. So that is a validity property.

So I need a distributed consensus protocol, which would provide me the agreement property as well as the validity property. And we have many well known distributed consensus protocol available, again, which is a very advanced application of cryptography.

(Refer Slide Time: 25:28)



Advanced Applications of Cryptography : VI

❑ Mutually distrusting parties $P_1, ..., P_n$

- ❖ P_i has a private input x_i
- ❖ A common n-ary function f

❑ Goals:

- ❖ Correctness: Compute $f(x_1,x_2,..x_n)$
- ❖ Privacy: Nothing more should be revealed beyond what can be learnt by your own input and the function output

And the final advanced application of cryptography which I would like to discuss is kind of Holy Grail problem in cryptography or in secure distributed computing, which is called a secure multi party computation or MPC in short, the problem description is the following. Imagine we are given a set of n mutually distrusting parties who are present across different portions of the globe.

And they do not trust each other. So imagine the parties are denoted by P_1 to P_n and each party has some private data, it could be a bit, it could be a database, it could be any kind of data. And there is a common function F, which is an n-ary function by n-ary function, I mean the function takes input from the n entities. So the goal here is to come up with a protocol according to which the parties exchange messages with each other.

Such that at the end of the protocol, the following 2 goals should be achieved. The first goal is the correctness namely, the good guys should be able to obtain the output of the function on the inputs of all the parties, irrespective of the behavior of the bad guys, and the second important goal is that of privacy, which requires that the adversary or the bad guys should not learn anything during the protocol beyond what can be revealed from its own input and the function output.

So on a very high level, the goal of the MPC protocol is to emulate the effect of a trusted third party. Imagine for the moment you have a trusted third party available to all the n parties, then this problem of multi party computation is very easy to solve. What each party can do is it can send its input privately to the trusted third party. And since the third party is trusted by all the entities, we have the guarantee that it would not reveal the inputs of the individual person to the other parties.

Now, the trusted third party can compute the value of the function on all the n inputs, and it can send back the output to every entity. But the problem with the solution with the trusted part third party is that in practice, we do not have any such trusted third party available. So the goal of a secure multi party computation protocol is to emulate the role of a trusted third party by running a protocol among the entities itself.

That means what a secure multi party computation protocol guarantees for you is that whatever is doable in the presence of a trusted third party, the same can be achieved even in the absence of a trusted third party by running a protocol among the individual entities. So this is like the holy grail problem on secure distributed computing, because if you have a solution for this abstract problem, then you have solutions of thousands of real world problems which can be abstracted by this beautiful notion of secure multi party computation.

So, that brings me to the end of this first lecture. To conclude with in this lecture, we briefly discussed what cryptography is all about, the significance of cryptography, and we discussed some of the advanced applications of cryptography. I hope you enjoyed this lecture. Thank you.