"In peace prepare for war, in war prepare for peace. The art of war is of vital importance to the state. It is matter of life and death, a road either to safety or to ruin. Hence under no circumstances can it be neglected."

– 'The Art of War', Sun Tzu
(Spring and Autumn Period, 771 to 476 BCE)

Cryptography: What Should Be Used?

Palash Sarkar

Applied Statistics Unit
Indian Statistical Institute, Kolkata
India
palash@isical.ac.in

International Conference on Security Aspects in Information Technology, High-Performance Computing and Networking
22^{nd} October 2011

Book Ciphers

```
534 C2 13 127 36 31 4 17 21 41
DOUGLAS 109 293 5 37 BIRLSTONE
26 BIRLSTONE 9 47 171
```

– ‘Valley of Fear’, Arthur Conan Doyle

Book Ciphers

```
534 C2 13 127 36 31 4 17 21 41
DOUGLAS 109 293 5 37 BIRLSTONE
26 BIRLSTONE 9 47 171
```

– ‘Valley of Fear’, Arthur Conan Doyle

- Secure?
  - No generic attacks: Depends on whether the book (and other parameters which constitute the key) can be guessed.
  - Does not provide authentication: truncation, mix-n-match attacks.

Book Ciphers

```
534 C2 13 127 36 31 4 17 21 41
DOUGLAS 109 293 5 37 BIRLSTONE
26 BIRLSTONE 9 47 171
```

– ‘Valley of Fear’, Arthur Conan Doyle

- Secure?
  - No generic attacks: Depends on whether the book (and other parameters which constitute the key) can be guessed.
  - Does not provide authentication: truncation, mix-n-match attacks.
- Easy-to-use? No! Secretly carrying around large books is not convenient.
  - Solution: Distribute the book digitally.
  - Circularity: Should the digital copy be encrypted? With what?

Book Ciphers

```
534 C2 13 127 36 31 4 17 21 41
DOUGLAS 109 293 5 37 BIRLSTONE
26 BIRLSTONE 9 47 171
```

– 'Valley of Fear', Arthur Conan Doyle

- Secure?
  - No generic attacks: Depends on whether the book (and other parameters which constitute the key) can be guessed.
  - Does not provide authentication: truncation, mix-n-match attacks.
- Easy-to-use? No! Secretly carrying around large books is not convenient.
  - Solution: Distribute the book digitally.
  - Circularity: Should the digital copy be encrypted? With what?

Should book ciphers be used for serious cryptography in the modern age?

Are there any advantages of book ciphers over one-time pad?

Ciphers Up To WW-II

- *Pre-twentieth century*: **Substitution**, **Permutation**, **Vigenére**,...
  - Evolution from mono-alphabetic to poly-alphabetic ciphers.
  - Cumbersome: tedious and inconvenient to encrypt and decrypt.
  - Cryptanalysis: from simple frequency analysis to more sophisticated statistical analysis.

Ciphers Up To WW-II

- *Pre-twentieth century*: **Substitution**, **Permutation**, **Vigenére**,...
  - Evolution from mono-alphabetic to poly-alphabetic ciphers.
  - Cumbersome: tedious and inconvenient to encrypt and decrypt.
  - Cryptanalysis: from simple frequency analysis to more sophisticated statistical analysis.
- *'Mechanisation of secrecy'* (cf. Simon Singh): **Enigma**, **Lorenz**,...
  - Encrypting and decrypting became fast, reliable and convenient.
  - The possibility of using machines also introduced the possibility of adding security features which were previously unthinkable.

Ciphers Up To WW-II

- *Pre-twentieth century*: **Substitution**, **Permutation**, **Vigenére**,...
  - Evolution from mono-alphabetic to poly-alphabetic ciphers.
  - Cumbersome: tedious and inconvenient to encrypt and decrypt.
  - Cryptanalysis: from simple frequency analysis to more sophisticated statistical analysis.
- *'Mechanisation of secrecy'* (cf. Simon Singh): **Enigma**, **Lorenz**,...
  - Encrypting and decrypting became fast, reliable and convenient.
  - The possibility of using machines also introduced the possibility of adding security features which were previously unthinkable.
- 'Mechanisation of secrecy' defeated by *mechanisation of cryptanalysis*.
  - Enigma by **Bombe**; Lorenz by **Colossus**.

Digitisation of Information

Ushered in a silent paradigm shift.

- All information (text, pictures, voices, ...) are bit sequences.
  - The linguistic connection to cryptology got severed.

Digitisation of Information

Ushered in a silent paradigm shift.

- All information (text, pictures, voices, ...) are bit sequences.
  - The linguistic connection to cryptology got severed.

Pre-dominant role of computers.

- Major advances in computer/communication engineering.
- Miniaturisation and ubiquitousness of computing facilities.
- Each new segment of digitisation has brought with it associated cryptographic problems.

Digitisation of Information

Ushered in a silent paradigm shift.

- All information (text, pictures, voices, ...) are bit sequences.
  - The linguistic connection to cryptology got severed.

Pre-dominant role of computers.

- Major advances in computer/communication engineering.
- Miniaturisation and ubiquitousness of computing facilities.
- Each new segment of digitisation has brought with it associated cryptographic problems.

Flow of mathematical ideas.

- Further development of ideas for statistical cryptanalysis.
- Use of discrete probability for defining and arguing about security.
- Application of computational complexity theory to quantify cryptanalytic effort.
- Machinery from algebra and number theory for building cryptographic systems.
- Concomitant development of coding theory.

Overview of the Talk

- Security requirements and cryptographic primitives.
- Between proprietary and public-domain algorithms.
- Crypto-technology development and deployment: a socio-economic model.

Security Requirements and Cryptographic Primitives

One-Time Pad and Authentication

One-time pad provides perfect secrecy.

One-Time Pad and Authentication

One-time pad provides perfect secrecy.

- Consider message: **attack at dawn**.
- Let $\mathbf{y}_1||\mathbf{y}_2$ be the ciphertext under one-time pad where,
  - $\mathbf{y}_1$ is the encryption of **attack**.
  - $\mathbf{y}_2$ is the encryption of **at dawn**.
- Then $\mathbf{y}_1$ itself is a valid forgery.
- If the adversary can successfully truncate the message, then a field unit may be lead into believing that the order is to attack immediately.

One-Time Pad and Authentication

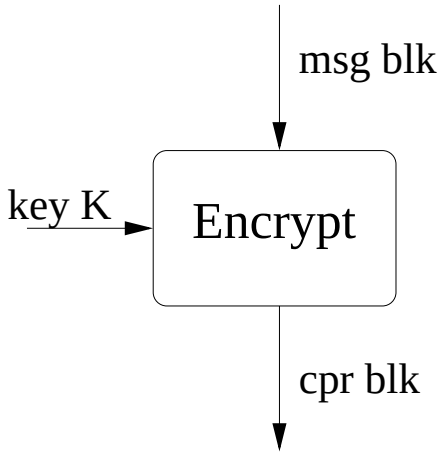
One-time pad provides perfect secrecy.

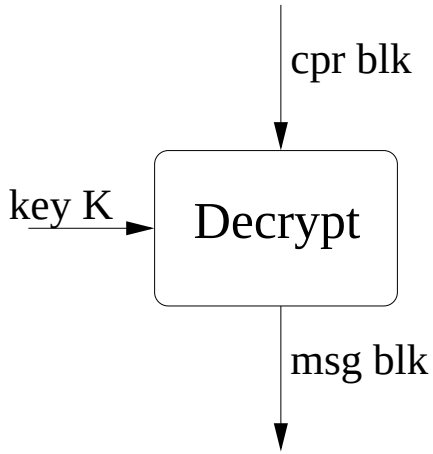
- Consider message: **attack at dawn**.
- Let $\mathbf{y}_1||\mathbf{y}_2$ be the ciphertext under one-time pad where,
  - $\mathbf{y}_1$ is the encryption of **attack**.
  - $\mathbf{y}_2$ is the encryption of **at dawn**.
- Then $\mathbf{y}_1$ itself is a valid forgery.
- If the adversary can successfully truncate the message, then a field unit may be lead into believing that the order is to attack immediately.

One-time pad does not provide authentication.

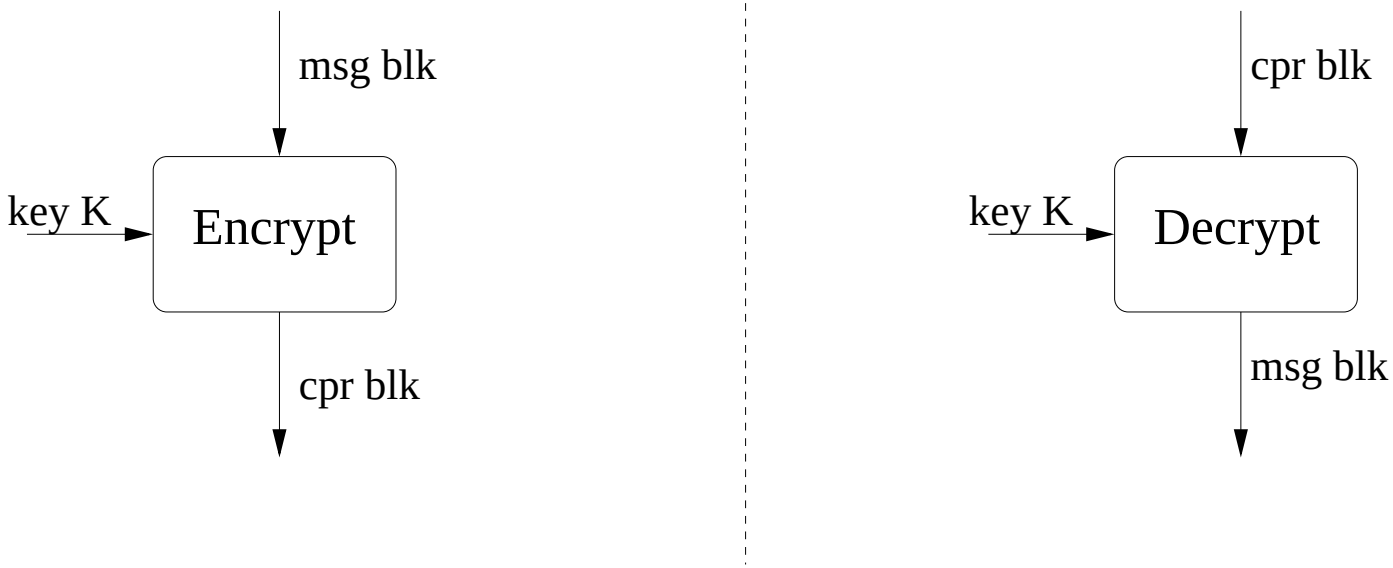
Moral: secure encryption does not imply secure authentication.

Encrypting Short Fixed Length Strings





Encrypting Short Fixed Length Strings

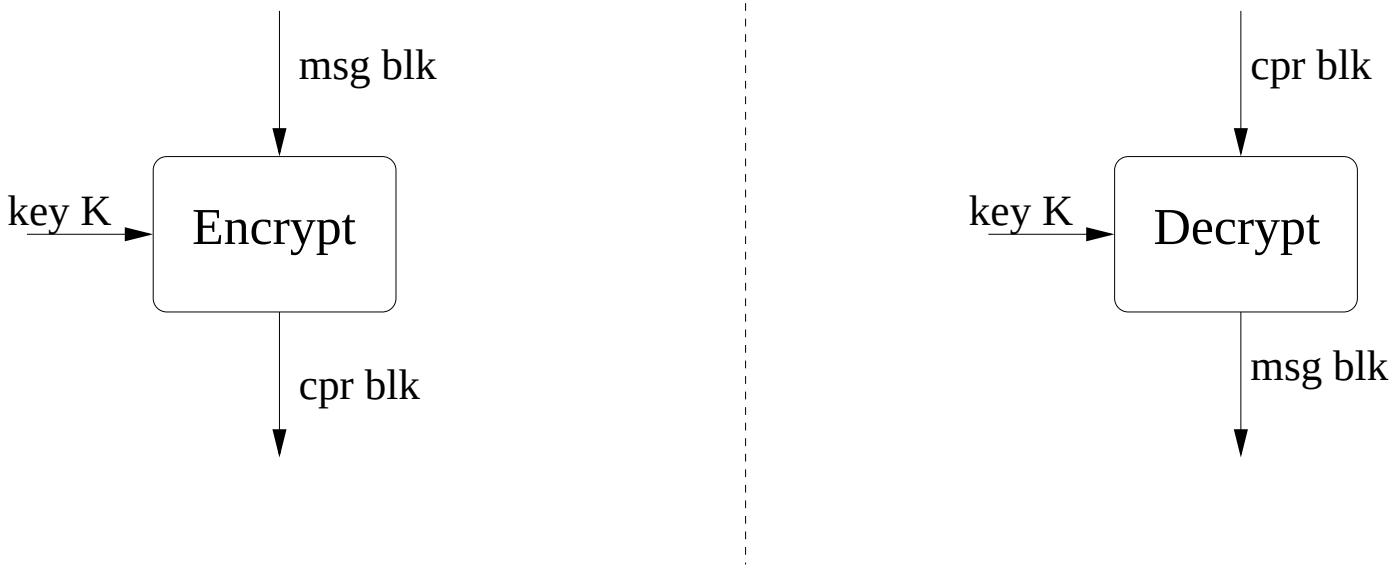


How Far Does a Block Cipher Take You?

Assumption: the block cipher is “perfectly secure” (whatever that may mean).

Is that the end of the story?

Encrypting Short Fixed Length Strings



How Far Does a Block Cipher Take You?

Assumption: the block cipher is “perfectly secure” (whatever that may mean).

Is that the end of the story?

No!

Block Cipher and Various Requirements

Message Requirements.

- A block cipher handles n-bit blocks: typically, $n = 128, 192$ or 256.
- Applications require handling “long” and/or “variable length” messages.

Block Cipher and Various Requirements

Message Requirements.

- A block cipher handles n-bit blocks: typically, $n = 128, 192$ or 256.
- Applications require handling “long” and/or “variable length” messages.

Security Requirements.

- A block cipher ensures strong security for n-bit blocks.
- Different Security Requirements.
  - Privacy.
  - Authentication.
  - Authenticated encryption.
  - Authenticated encryption with associated data.
  - Disk sector encryption.
  - Deterministic authenticated encryption (key wrap problem).
  - Format preserving encryption.

Mode of Operation

Extends the capability of a block cipher to handle “long’ strings.

Mode of Operation

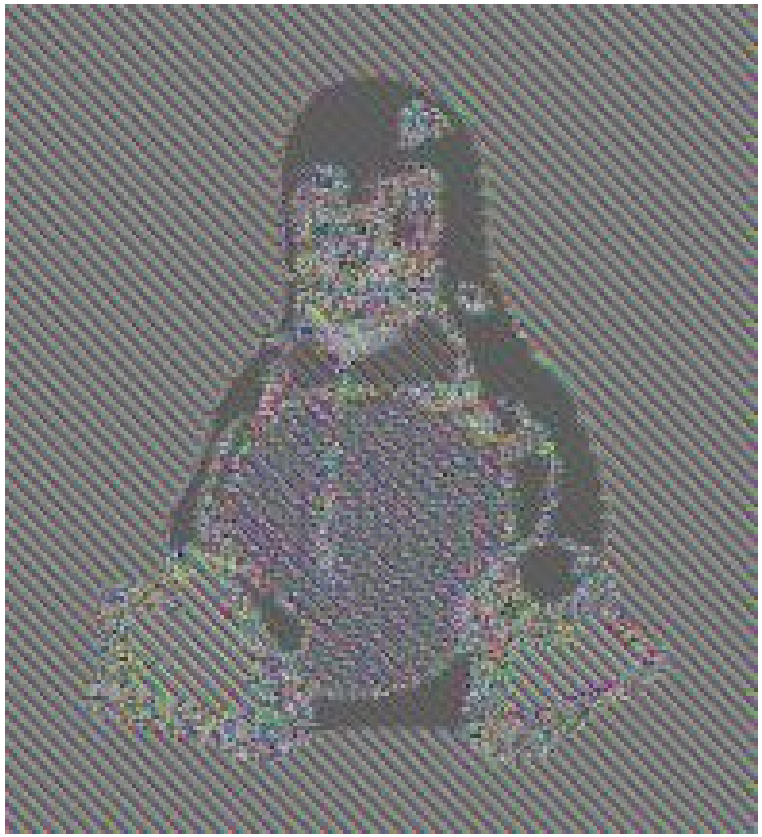
Extends the capability of a block cipher to handle “long’ strings.

Basic modes.

- Electronic codebook mode (ECB).
- Counter mode (Ctr).
- Cipher block chaining mode (CBC).
- Output feedback mode (OFB).
- Cipher feedback mode (CFB).

Insecurity of ECB Mode





Source: Wikipedia

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation.

Things to Note

- ECB does not provide privacy.
- Ctr provides privacy but not authentication.
- CBC provides authentication, but, not authenticated encryption.
- Authenticated encryption (with associated data)?
- Wide block encryption?
- Disk encryption?
- Other security requirements?

There is no single mode which can be used for all applications.

Other Primitives

Stream Cipher:

- Without IV: Modelled as a PRG.
  With IV: Modelled as a PRF.
- Questions:
  - How to achieve authentication?
  - How to achieve authenticated encryption (with associated data), ...?

Other Primitives

Stream Cipher:

- Without IV: Modelled as a PRG.
  With IV: Modelled as a PRF.
- Questions:
  - How to achieve authentication?
  - How to achieve authenticated encryption (with associated data), ...?

Hash Function:

- What is the property that one requires for a particular application?
  Note: HMAC achieves authentication even without collision-resistance.
- General hash functions are often considered to be the crypto-equivalent of swiss army knife. But, for any particular application, it is important to know exactly what assumption one requires of a hash function.

To Be Or Not To Be Proprietary?

Security-by-obscurity versus Kerckhoff's principle

If you do not know it, you cannot break it.

Versus

"The enemy knows the system." (Shannon)

Security-by-obscurity versus Kerckhoff's principle

If you do not know it, you cannot break it.

Versus

"The enemy knows the system." (Shannon)

Kerckhoff's principle (1883): The only secret is the key.

Security-by-obscurity versus Kerckhoff's principle

One side of the argument:

- There are 'incentives' for the disclosure of a crypto-system.
  - Is it acceptable to use a system whose weaknesses may be exposed if the system becomes known?
- Ostrich effect.
  - Should one not use crypto tools developed by the general scientific community?

Security-by-obscurity versus Kerckhoff's principle

One side of the argument:

- There are 'incentives' for the disclosure of a crypto-system.
  - Is it acceptable to use a system whose weaknesses may be exposed if the system becomes known?
- Ostrich effect.
  - Should one not use crypto tools developed by the general scientific community?

The other side:

- Using public domain algorithms.
  - How does one know/verify that there are no 'hidden' weaknesses?

Security-by-obscurity versus Kerckhoff's principle

One side of the argument:

- There are 'incentives' for the disclosure of a crypto-system.
  - Is it acceptable to use a system whose weaknesses may be exposed if the system becomes known?
- Ostrich effect.
  - Should one not use crypto tools developed by the general scientific community?

The other side:

- Using public domain algorithms.
  - How does one know/verify that there are no 'hidden' weaknesses?
- "You can't trust code that you did not create yourself."

'Reflections on Trusting Trust'
– Ken Thompson's Turing award lecture (1983).

Security-by-obscurity versus Kerckhoff's principle

One side of the argument:

- There are 'incentives' for the disclosure of a crypto-system.
  - Is it acceptable to use a system whose weaknesses may be exposed if the system becomes known?
- Ostrich effect.
  - Should one not use crypto tools developed by the general scientific community?

The other side:

- Using public domain algorithms.
  - How does one know/verify that there are no 'hidden' weaknesses?
- "You can't trust code that you did not create yourself."

'Reflections on Trusting Trust'
– Ken Thompson's Turing award lecture (1983).

The two sides are not necessarily contradictory; they may even be complementary.

Security-by-obscurity versus Kerckhoff's principle

- Symmetric-key ciphers: It is possible to use security-by-obscurity as a secondary security measure in the deployment of cryptographic algorithms.
  - Pick a random secret cipher from a 'large' family of well-studied ciphers.
  - Open-domain 'third-party cryptanalysis' verifies that all ciphers in the family have the same security level.

Security-by-obscurity versus Kerckhoff's principle

- Symmetric-key ciphers: It is possible to use security-by-obscurity as a secondary security measure in the deployment of cryptographic algorithms.
  - Pick a random secret cipher from a 'large' family of well-studied ciphers.
  - Open-domain 'third-party cryptanalysis' verifies that all ciphers in the family have the same security level.
- Trust in a crypto product cannot be stronger than the trust in the people who built it.
  - It is not possible to 'buy' trust from unknown/untrusted parties.
  - Trust is linked to (economic) incentives and disincentives.
  - There is need for a viable (dis)incentive-based trust model for multi-organisational development of crypto products.
  - 'Trust-mapping' of a crypto-product: trust in the organisations which have been involved in developing the product.

Public-Key Cryptography

- Evolution: Use of radio lead to a huge amount of communication.
  - For any communication to be useful, it must be secure.
  - It became very difficult to handle key management issues using conventional cryptographic methods.

Public-Key Cryptography

- Evolution: Use of radio lead to a huge amount of communication.
  - For any communication to be useful, it must be secure.
  - It became very difficult to handle key management issues using conventional cryptographic methods.
- Birth of PKE: (‘Necessity is the mother of invention’ – Plato.)
  - Concomitant ‘cultural revolution’ in the attitude to cryptology as a science.
  - Issues of trust-related pitfalls leading to public-key infrastructure evolving into the formulation of identity-based encryption.
  - Proprietary PKE: The GCHQ story.

Public-Key Cryptography

- Evolution: Use of radio lead to a huge amount of communication.
  - For any communication to be useful, it must be secure.
  - It became very difficult to handle key management issues using conventional cryptographic methods.
- Birth of PKE: (‘Necessity is the mother of invention’ – Plato.)
  - Concomitant ‘cultural revolution’ in the attitude to cryptology as a science.
  - Issues of trust-related pitfalls leading to public-key infrastructure evolving into the formulation of identity-based encryption.
  - Proprietary PKE: The GCHQ story.

Policy issue: Should one use public-key cryptography?

- Creation of secure channels between (hundreds of) thousands of users: How to handle the key management issue?

Public-Key Cryptography

- Evolution: Use of radio lead to a huge amount of communication.
  - For any communication to be useful, it must be secure.
  - It became very difficult to handle key management issues using conventional cryptographic methods.
- Birth of PKE: (‘Necessity is the mother of invention’ – Plato.)
  - Concomitant ‘cultural revolution’ in the attitude to cryptology as a science.
  - Issues of trust-related pitfalls leading to public-key infrastructure evolving into the formulation of identity-based encryption.
  - Proprietary PKE: The GCHQ story.

Policy issue: Should one use public-key cryptography?

- Creation of secure channels between (hundreds of) thousands of users: How to handle the key management issue?
- Digital Signatures, Information Technology Act, E-Commerce, ... (Another story).

Information-Theoretic Cryptography

- One-time pad: provides perfect secrecy for encryption.
- Universal hash function:
  - Polynomial hash, multi-linear hash, UMAC, ...

Information-Theoretic Cryptography

- One-time pad: provides perfect secrecy for encryption.
- Universal hash function:
  - Polynomial hash, multi-linear hash, UMAC, ...
- Modes of operations of a block cipher:
  - Assumes the underlying block cipher to be a ideal primitive.
  - Provides a proof that a mode is secure in an appropriate sense.
  - Works the same way irrespective of whether the underlying block cipher is proprietary or public-domain.
- Modes of operations of a hash function:
  - Merkle-Damgärd structure.
  - Indifferentiability analysis.

Information-Theoretic Cryptography

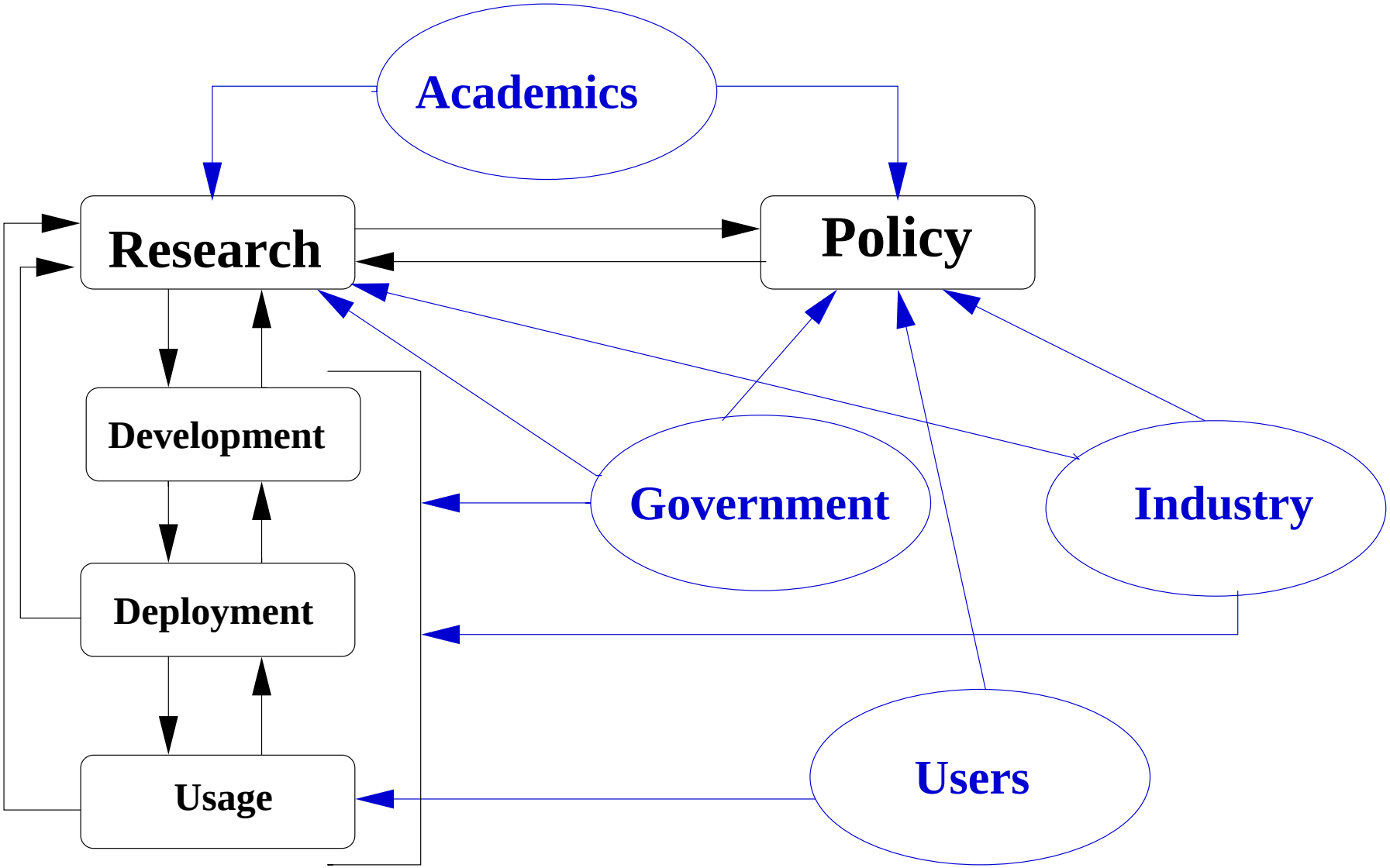
- One-time pad: provides perfect secrecy for encryption.
- Universal hash function:
  - Polynomial hash, multi-linear hash, UMAC, ...
- Modes of operations of a block cipher:
  - Assumes the underlying block cipher to be a ideal primitive.
  - Provides a proof that a mode is secure in an appropriate sense.
  - Works the same way irrespective of whether the underlying block cipher is proprietary or public-domain.
- Modes of operations of a hash function:
  - Merkle-Damgärd structure.
  - Indifferentiability analysis.

Should one avoid using information-theoretic cryptography simply because it is in the public domain?

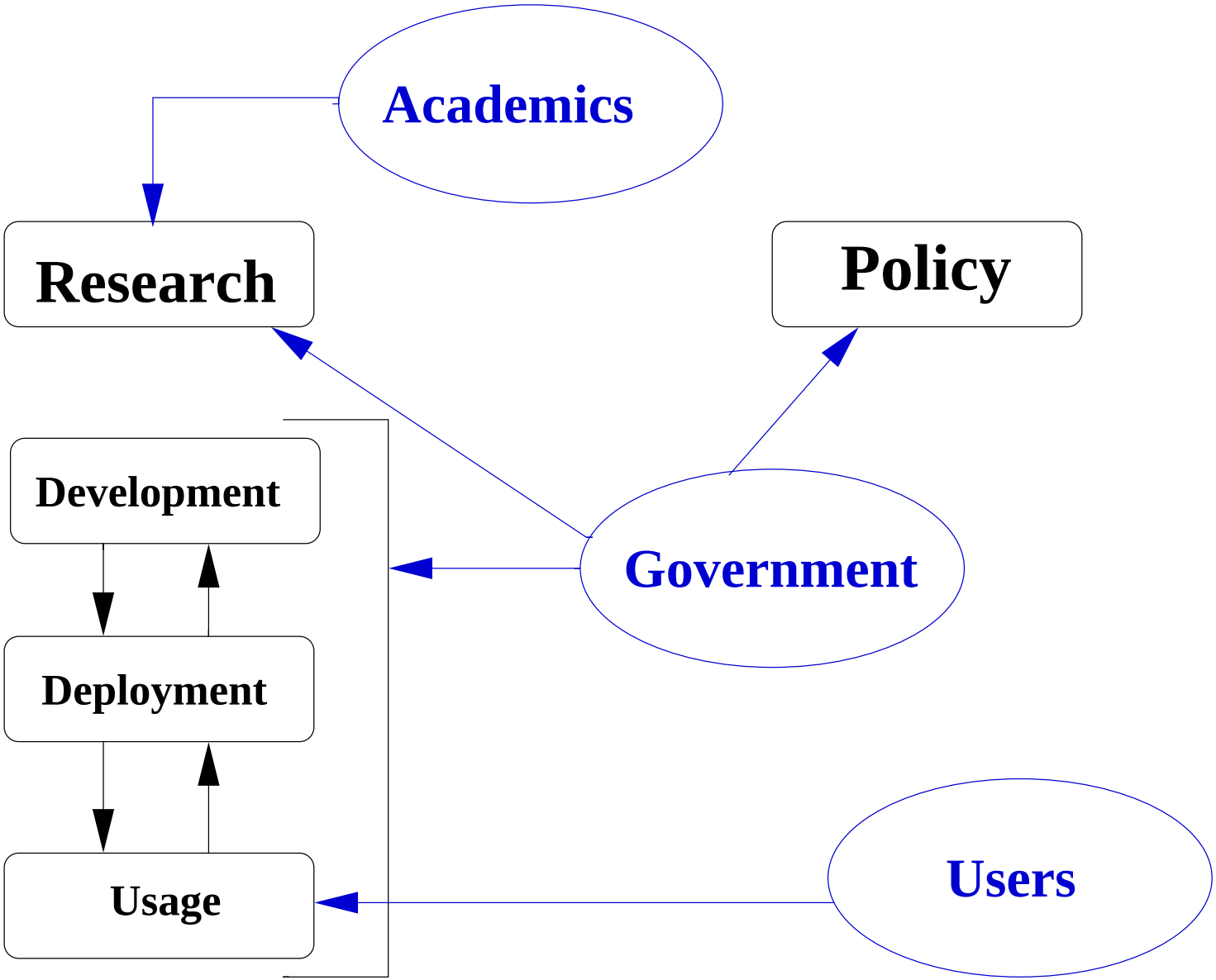
Crypto-Technology Development and Deployment:

A Socio-Economic Model

Stake-Holders and Activities: ‘Ideal Model’



Missing Links: Indian Context



Assets, Costs and Values

- Assets requiring cryptographic protection.
  - Information: privacy and/or integrity.
  - Commitments, goodwill, ...
  - Asset mapping: identify assets and their relationships.

Assets, Costs and Values

- Assets requiring cryptographic protection.
  - Information: privacy and/or integrity.
  - Commitments, goodwill, ...
  - Asset mapping: identify assets and their relationships.

  Costs.
  - Cost of generating the asset.
  - Value to adversaries; possibly varies with adversaries.

Assets, Costs and Values

- Assets requiring cryptographic protection.
  - Information: privacy and/or integrity.
  - Commitments, goodwill, ...
  - Asset mapping: identify assets and their relationships.

  Costs.
  - Cost of generating the asset.
  - Value to adversaries; possibly varies with adversaries.
- Adversarial cost/value.
  - Cost of a cryptanalytic attempt.
  - The pay-off on success is the value to the adversary.

Assets, Costs and Values

- Assets requiring cryptographic protection.
  - Information: privacy and/or integrity.
  - Commitments, goodwill, ...
  - Asset mapping: identify assets and their relationships.

  Costs.
  - Cost of generating the asset.
  - Value to adversaries; possibly varies with adversaries.
- Adversarial cost/value.
  - Cost of a cryptanalytic attempt.
  - The pay-off on success is the value to the adversary.
- Cost of deployment of cryptographic measures.
  - Depends on the (estimated) adversarial value of the resource.

Assets, Costs and Values

- Assets requiring cryptographic protection.
  - Information: privacy and/or integrity.
  - Commitments, goodwill, ...
  - Asset mapping: identify assets and their relationships.

  Costs.
  - Cost of generating the asset.
  - Value to adversaries; possibly varies with adversaries.
- Adversarial cost/value.
  - Cost of a cryptanalytic attempt.
  - The pay-off on success is the value to the adversary.
- Cost of deployment of cryptographic measures.
  - Depends on the (estimated) adversarial value of the resource.
- Cryptographic and cryptanalytic costs.
  - Cost for attaining the immediate objective.
  - Long-term cost for capability acquisition.

Assets, Costs and Values

- Assets requiring cryptographic protection.
  - Information: privacy and/or integrity.
  - Commitments, goodwill, ...
  - Asset mapping: identify assets and their relationships.

  Costs.
  - Cost of generating the asset.
  - Value to adversaries; possibly varies with adversaries.
- Adversarial cost/value.
  - Cost of a cryptanalytic attempt.
  - The pay-off on success is the value to the adversary.
- Cost of deployment of cryptographic measures.
  - Depends on the (estimated) adversarial value of the resource.
- Cryptographic and cryptanalytic costs.
  - Cost for attaining the immediate objective.
  - Long-term cost for capability acquisition.

All costs and values are time-dependent.

Do People Understand?

Example: Browsers flash a message about 128-bit security.

- Do users understand what this is about?
- A user will know a lot about his favourite film star: but, what about his requirements of cryptographic protection?

Do People Understand?

Example: Browsers flash a message about 128-bit security.

- Do users understand what this is about?
- A user will know a lot about his favourite film star: but, what about his requirements of cryptographic protection?

Example: In India, digital certificates are required to be purchased by railway ticketing agents.

- Do the agents understand why they need a certificate?
- Do the customers understand how the certificate is related to their protection?

Do People Understand?

Example: Browsers flash a message about 128-bit security.

- Do users understand what this is about?
- A user will know a lot about his favourite film star: but, what about his requirements of cryptographic protection?

Example: In India, digital certificates are required to be purchased by railway ticketing agents.

- Do the agents understand why they need a certificate?
- Do the customers understand how the certificate is related to their protection?

Civil liberties groups: Create user consciousness about cryptographic needs.

- In 1998, EFF built a DES cracker to underline the point that 56-bit keys can be exhaustively searched.

Who Needs Cryptography?

- Government: To ensure common good, a government requires cryptography for different affairs of the state.
- General public: The extent of cryptographic requirement is strongly correlated to economic strata.

Who Needs Cryptography?

- Government: To ensure common good, a government requires cryptography for different affairs of the state.
- General public: The extent of cryptographic requirement is strongly correlated to economic strata.

Types of consumers of crypto-technology.

- Sensitised.
  - Cryptographic needs are directly assessed by the users themselves.
  - Methods are pro-actively acquired and deployed by the users themselves.
- Unsensitised.
  - Cryptographic needs are assessed by others.
  - Protective mechanisms are deployed on behalf of the user.
  - 'Cryptographic Fool's Paradise':
    No knowledge or understanding of one's cryptographic needs and protection mechanisms that are deployed on one's behalf.

Attack Goals

- Direct: Defeat strong cryptography deployed by knowledgeable users/organisations.
- Indirect: Defeat users with poor understanding and/or poor cryptographic protection.
  - Vulnerability analysis identifies such weak points.

Attack Goals

- Direct: Defeat strong cryptography deployed by knowledgeable users/organisations.
- Indirect: Defeat users with poor understanding and/or poor cryptographic protection.
  - Vulnerability analysis identifies such weak points.
- Spread-Out: Defeat a large number of individuals having weak (or no) cryptographic protection.
  - *Example:* steal a small amount of money from a large number of credit cards.
  - Maxim: Take little from many.

Attack Goals

- Direct: Defeat strong cryptography deployed by knowledgeable users/organisations.
- Indirect: Defeat users with poor understanding and/or poor cryptographic protection.
  - Vulnerability analysis identifies such weak points.
- Spread-Out: Defeat a large number of individuals having weak (or no) cryptographic protection.
  - *Example:* steal a small amount of money from a large number of credit cards.
  - Maxim: Take little from many.
- Trust structure of an organisation.
  - How much cryptography is required by whom?
  - What is the ripple effect of trust failure at a point?

Attack Goals

- Direct: Defeat strong cryptography deployed by knowledgeable users/organisations.
- Indirect: Defeat users with poor understanding and/or poor cryptographic protection.
  - Vulnerability analysis identifies such weak points.
- Spread-Out: Defeat a large number of individuals having weak (or no) cryptographic protection.
  - *Example:* steal a small amount of money from a large number of credit cards.
  - Maxim: Take little from many.
- Trust structure of an organisation.
  - How much cryptography is required by whom?
  - What is the ripple effect of trust failure at a point?

A cryptographer should be interested in everything (and only those things) that adversaries of the present and the future are interested in.

Do Organisations Take Their Crypto Seriously?

- Detailed descriptions of resources that require protection.
  - Consideration of different aspects of data on the move, at rest, ...
  - Modelling relationships among sensitive resources can be a complex task.

Do Organisations Take Their Crypto Seriously?

- Detailed descriptions of resources that require protection.
  - Consideration of different aspects of data on the move, at rest, ...
  - Modelling relationships among sensitive resources can be a complex task.
- Adversarial mapping.
  - Who/What are the adversaries and the value of different resources to different adversaries.

Do Organisations Take Their Crypto Seriously?

- Detailed descriptions of resources that require protection.
  - Consideration of different aspects of data on the move, at rest, ...
  - Modelling relationships among sensitive resources can be a complex task.
- Adversarial mapping.
  - Who/What are the adversaries and the value of different resources to different adversaries.
- Regular audit of deployed cryptographic mechanisms.
- Consideration of active protection using cryptanalytic techniques.

Do Organisations Take Their Crypto Seriously?

- Detailed descriptions of resources that require protection.
  - Consideration of different aspects of data on the move, at rest, ...
  - Modelling relationships among sensitive resources can be a complex task.
- Adversarial mapping.
  - Who/What are the adversaries and the value of different resources to different adversaries.
- Regular audit of deployed cryptographic mechanisms.
- Consideration of active protection using cryptanalytic techniques.

Finance is important enough to have a Chief Finance Office.
Is Cryptology important enough to have a Chief Cryptology Officer?

Crypto-Technology: Industry Stimulus

- Growth of crypto industry.
  - *Sensitised* users clamour for cryptographic protection.
  - Creates demand for crypto-technology.
  - Industry expands to supply products.

Crypto-Technology: Industry Stimulus

- Growth of crypto industry.
  - *Sensitised* users clamour for cryptographic protection.
  - Creates demand for crypto-technology.
  - Industry expands to supply products.
- Acquiring cryptographic/cryptanalytic capability is a long-term investment.
  - Requires top-quality equipments.
  - Requires highly skilled (and hence highly paid) human resources.
  - For attaining depth in research, an organisation has to build cryptanalytic capability along with cryptographic capability.

Crypto-Technology: Industry Stimulus

- Growth of crypto industry.
  - *Sensitised* users clamour for cryptographic protection.
  - Creates demand for crypto-technology.
  - Industry expands to supply products.
- Acquiring cryptographic/cryptanalytic capability is a long-term investment.
  - Requires top-quality equipments.
  - Requires highly skilled (and hence highly paid) human resources.
  - For attaining depth in research, an organisation has to build cryptanalytic capability along with cryptographic capability.
- Can industry take up classified work for the government?
  - Policy issues: granting of licences; regular "trust audit" of procedures and people.
  - Drawing the line: so far and no further.

Crypto-Technology: Industry Stimulus

- Growth of crypto industry.
  - *Sensitised* users clamour for cryptographic protection.
  - Creates demand for crypto-technology.
  - Industry expands to supply products.
- Acquiring cryptographic/cryptanalytic capability is a long-term investment.
  - Requires top-quality equipments.
  - Requires highly skilled (and hence highly paid) human resources.
  - For attaining depth in research, an organisation has to build cryptanalytic capability along with cryptographic capability.
- Can industry take up classified work for the government?
  - Policy issues: granting of licences; regular "trust audit" of procedures and people.
  - Drawing the line: so far and no further.

Crypto-industry in India is a sleeping giant.

(Policy changes and user education required to awaken it.)

Need for a National Cryptologic Plan

- Policy formulation with well-defined goals.

Need for a National Cryptologic Plan

- Policy formulation with well-defined goals.
- Based on current and evolving socio-economic reality.
  - Model of the sixties will not be successful today.
- Based on inclusive discussion among all the stake-holders.
  - Government, industry, users and academics.

Need for a National Cryptologic Plan

- Policy formulation with well-defined goals.
- Based on current and evolving socio-economic reality.
  - Model of the sixties will not be successful today.
- Based on inclusive discussion among all the stake-holders.
  - Government, industry, users and academics.
- Ensure healthy interaction between different aspects of crypto activity.
  - Policy planning, research, development, deployment and usage.

Need for a National Cryptologic Plan

- Policy formulation with well-defined goals.
- Based on current and evolving socio-economic reality.
  - Model of the sixties will not be successful today.
- Based on inclusive discussion among all the stake-holders.
  - Government, industry, users and academics.
- Ensure healthy interaction between different aspects of crypto activity.
  - Policy planning, research, development, deployment and usage.
- Adopt with care public domain cryptography.
  - Internationally, the genie (of public-domain cryptography) is out of the bottle and cannot be put back in.

Need for a National Cryptologic Plan

- Policy formulation with well-defined goals.
- Based on current and evolving socio-economic reality.
  - Model of the sixties will not be successful today.
- Based on inclusive discussion among all the stake-holders.
  - Government, industry, users and academics.
- Ensure healthy interaction between different aspects of crypto activity.
  - Policy planning, research, development, deployment and usage.
- Adopt with care public domain cryptography.
  - Internationally, the genie (of public-domain cryptography) is out of the bottle and cannot be put back in.
- Stimulate the growth of crypto-industry by adopting with care an appropriate public-private partnership model.
  - In today's world, government activity alone is not enough for national development of cryptology.

Need for a National Cryptologic Plan

- Policy formulation with well-defined goals.
- Based on current and evolving socio-economic reality.
  - Model of the sixties will not be successful today.
- Based on inclusive discussion among all the stake-holders.
  - Government, industry, users and academics.
- Ensure healthy interaction between different aspects of crypto activity.
  - Policy planning, research, development, deployment and usage.
- Adopt with care public domain cryptography.
  - Internationally, the genie (of public-domain cryptography) is out of the bottle and cannot be put back in.
- Stimulate the growth of crypto-industry by adopting with care an appropriate public-private partnership model.
  - In today's world, government activity alone is not enough for national development of cryptology.

National security is based on national trust network.

Summary

- Pre-modern cryptography.
- Some questions regarding whether a particular cryptographic primitive is suited for a particular task.
- Some questions regarding the adoption of cryptographic techniques developed in the public domain.
- A potpourri of broad issues which may affect the development of a national cryptologic plan.

Summary

- Pre-modern cryptography.
- Some questions regarding whether a particular cryptographic primitive is suited for a particular task.
- Some questions regarding the adoption of cryptographic techniques developed in the public domain.
- A potpourri of broad issues which may affect the development of a national cryptologic plan.

“But he isn’t wearing anything at all!”

– Emperor’s New Clothes
Hans Christian Andersen

An Analogy To Sun Tzu's Words

The science of cryptology is of vital importance to a nation. Failure of cryptographic mechanisms can have devastating consequences. Hence, no effort should be spared in acquiring the best possible cryptologic capability.

Thank you for your attention!