Course: Modern Cryptography

Key Management and the Public-Key Revolution

Shashank Singh

IISER Bhopal

October 24, 2025

Setting of Private-key Cryptography..

Classical Cryptography

- Before sending the message (plaintext) m, Alice transforms (encrypts) it into a message c (ciphertext), using an algorithm `ENC` and a key k.
- Bob, on receiving c, decrypts it to get m, using a corresponding algorithm `DEC` and the same key k.

Setting of Private-key Cryptography..

Classical Cryptography

- The key k, needs to be (somehow) shared between the two communicating parties in advance and it is not known to the adversary.

A Paradigm Shift

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems,**

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In

W. Diffie and M. Hellman

New directions in cryptography

IEEE Transactions on Information Theory- vol. 22, no. 6, pp. 644-654, Nov 1976..

of communications technology. Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing.

Manuscript received June 3, 1976. This work was partially supported by the National Science Foundation under NSF Grant ENG 10173. Portions of this work were presented at the IEEE Information Theory Workshop, Lenox, MA, June 23–25, 1975 and the IEEE International Symposium on Information Theory in Ronneby, Sweden, June 21–24, 1976.

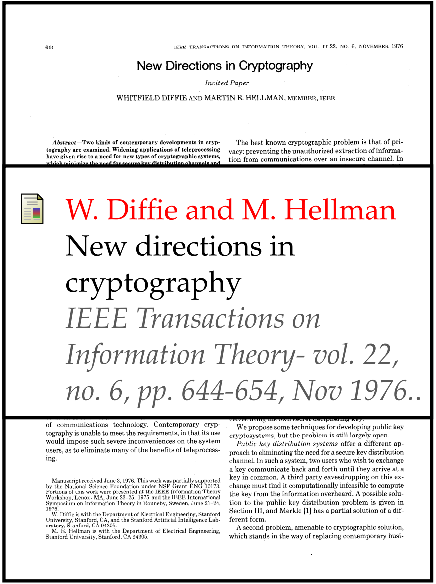
W. Diffie is with the Department of Electrical Engineering, Stanford University, Stanford, CA, and the Stanford Artificial Intelligence Laboratory, Stanford, CA 94305.
M. E. Hellman is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305.

We propose some techniques for developing public key cryptosystems, but the problem is still largely open.

Public key distribution systems offer a different approach to eliminating the need for a secure key distribution channel. In such a system, two users who wish to exchange a key communicate back and forth until they arrive at a key in common. A third party eavesdropping on this exchange must find it computationally infeasible to compute the key from the information overheard. A possible solution to the public key distribution problem is given in Section III, and Merkle [1] has a partial solution of a different form.

A second problem, amenable to cryptographic solution, which stands in the way of replacing contemporary busi-

A Paradigm Shift


644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems,**

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In

W. Diffie and M. Hellman

New directions in cryptography

IEEE Transactions on Information Theory- vol. 22, no. 6, pp. 644-654, Nov 1976..

of communications technology. Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing.

Manuscript received June 3, 1976. This work was partially supported by the National Science Foundation under NSF Grant ENG 10173. Portions of this work were presented at the IEEE Information Theory Workshop, Lenox, MA, June 23–25, 1975 and the IEEE International Symposium on Information Theory in Ronneby, Sweden, June 21–24, 1976.

W. Diffie is with the Department of Electrical Engineering, Stanford University, Stanford, CA, and the Stanford Artificial Intelligence Laboratory, Stanford, CA 94305.

M. E. Hellman is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305.

We propose some techniques for developing public key cryptosystems, but the problem is still largely open.

Public key distribution systems offer a different approach to eliminating the need for a secure key distribution channel. In such a system, two users who wish to exchange a key communicate back and forth until they arrive at a key in common. A third party eavesdropping on this exchange must find it computationally infeasible to compute the key from the information overheard. A possible solution to the public key distribution problem is given in Section III, and Merkle [1] has a partial solution of a different form.

A second problem, amenable to cryptographic solution, which stands in the way of replacing contemporary busi-

I. INTRODUCTION

We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and

...

In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels.

...

Onewayness

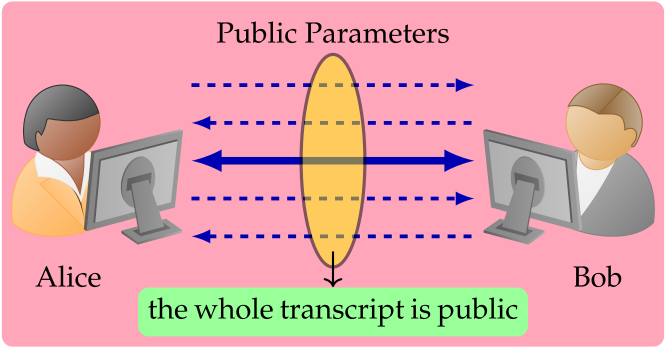
Diffie and Hellman observed certain asymmetries i.e., there are certain actions that can be easily performed but not easily reversed.

$p := \texttt{NextPrime}(2^{3000})$

$(\mathbb{Z}/p\mathbb{Z}^*, \odot)$ is a cyclic group. Let $(\mathbb{Z}/p\mathbb{Z}^*, \odot) = \langle g \rangle$.

- $(g, a) \to g^a$ is easy. (polynomial-time)
- $(g, h) \to \log_g(h)$ is hard. ((sub)exp.-time)

SETTING OF KEY-EXCHANGE PROTOCOL Π



☞ After the end of the protocol, both Alice and Bob comes up with keys k_A and k_B respectively such that $k_A = k_B = k$(say).

☞ Informally, the protocol is said to be secure if nobody other than Alice and Bob can have any idea about k.

The key-exchange experiment $\mathrm{KE}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n)$

- Two parties having n execute the protocol Π. This results in a transcript `trans` and a key k.
- $b \overset{\mathtt{uni}}{\leftarrow} \{0,1\}$. If $b = 0$, set $\hat{k} := k$, otherwise choose $\hat{k} \in \{0,1\}^n$ uniformly at random.
- $\mathcal{A}$ is given `trans` and $\hat{k}$. $\mathcal{A}$ outputs a bit b'.
- The output of experiment is defined to be 1 if $b' = b$ and 0 otherwise. If $\mathrm{KE}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n) = 1$, we say $\mathcal{A}$ succeeds.

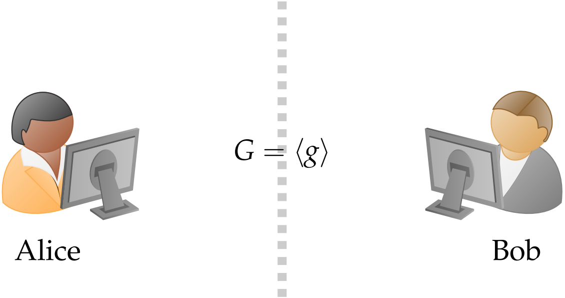
Definition

A key-exchange protocol Π is secure in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function ε such that

$$\Pr\left[\mathrm{KE}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \varepsilon(n)$$

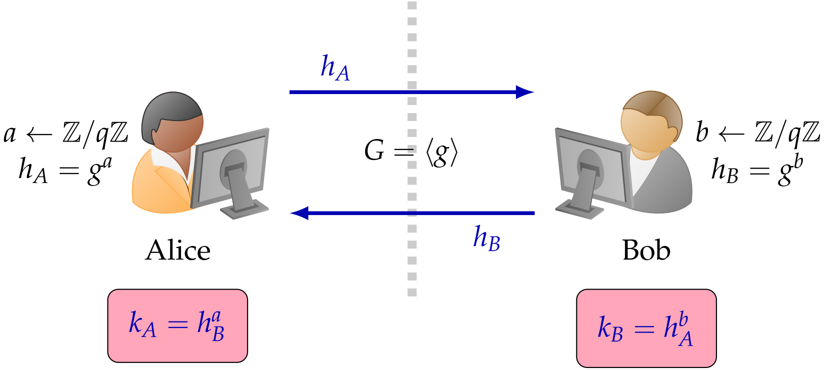
DIFFIE-HELLMAN KEY AGREEMENT PROTOCOL

Let $(G, .)$ be a cyclic group, where DLP is known to be computationally hard. Let $G = \langle g \rangle$ and $|G| = q$.



Diffie-Hellman Key Agreement Protocol

Let $(G, .)$ be a cyclic group, where DLP is known to be computationally hard. Let $G = \langle g \rangle$ and $|G| = q$.



Let $\widehat{\mathrm{KE}}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n)$ denote a modified experiment where if $b = 1$ the adversary is given $\hat{k}$ chosen uniformly from G instead of a uniform n-bit string.

Theorem

If the decisional Diffie-Hellman problem is hard relative to G, then the Diffie–Hellman key-exchange protocol Π is secure in the presence of an eavesdropper (with respect to the modified experiment $\widehat{\mathrm{KE}}^{\mathtt{eav}}_{\mathcal{A},\Pi}(n)$).

Proof.

Refer to the book. $\square$

Other attacks on Key Exacnage Protocols

– Impersonation attacks

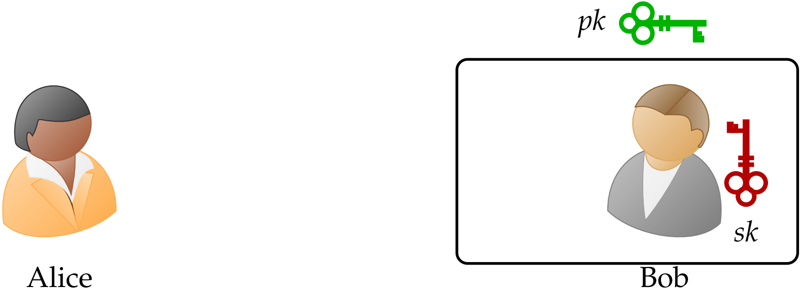
– Human(machine)-in-the-middle attacks

☞ The Diffie-Hellman Key exchange protocol is completely insecure against man-in-the-middle attacks.

Q1: If it is feasible to do the key exchange, why can't we send the entire message in the same way, eliminating the need for private key cryptography?

☞ Diffie and Hellman also introduced in their ground-breaking work the notion of public-key (or asymmetric) cryptography.

Setting of Public Key Cryptography



Setting of Public Key Cryptography