Keamanan Siber

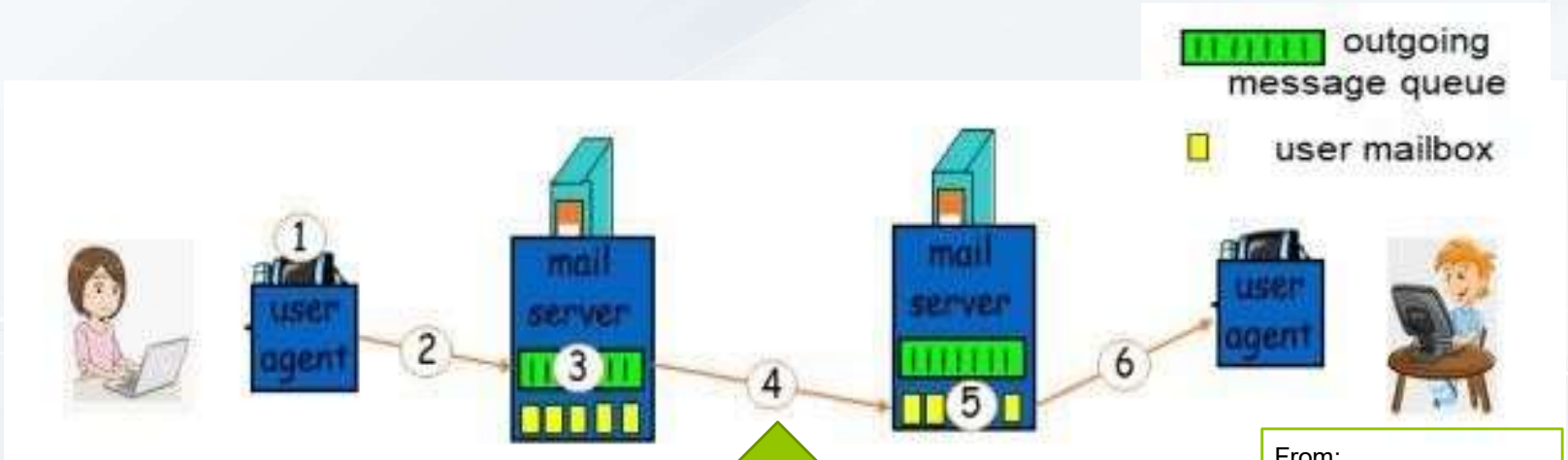
Pertemuan # Email Security

Always The First

Pendahuluan

- Surat elektronik, atau disingkat **Email**, adalah layanan jaringan yang paling banyak digunakan dan dihargai.
- Saat ini, isi pesan tidak aman:
  - Dapat diperiksa selama dalam perjalanan
  - Atau oleh pengguna dengan hak istimewa pada sistem tujuan

Langkah Dasar pada Email



To:
bob@someschool.com

From:
alice@somedomain.com

Sender mail server

SMTP

Receiver mail server

From:
alice@somedomain.com

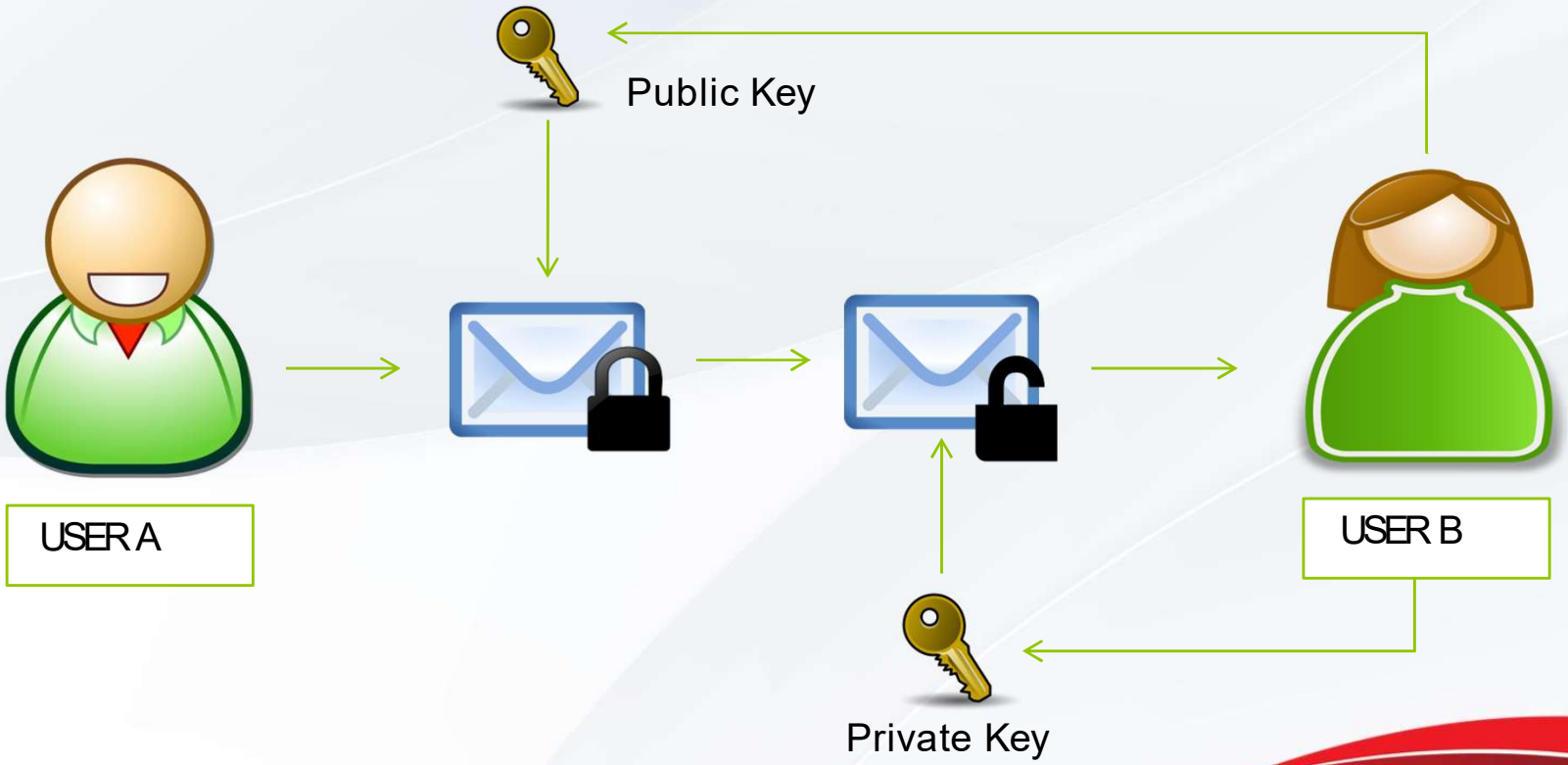
Email Security

- Teknik untuk melindungi akun email, konten, dan komunikasi dari akses, kehilangan, atau kompromi yang tidak sah.
- Melibatkan enkripsi konten pesan email untuk melindungi informasi yang mungkin sensitif agar tidak dibaca oleh siapa pun selain penerima yang dituju.

Ancaman Keamanan Email

- **Malware** – singkatan dari "*malicious software*" (perangkat lunak berbahaya).
- **Spam** – Email komersial yang tidak diminta.
- **Phishing** – Berhubungan dengan spam dalam beberapa hal.
- **Social Engineering** – Salah satu serangan rekayasa sosial yang umum adalah pemalsuan email (email spoofing).
- Masih banyak lagi…

Kerja Email Security



Kebutuhan Keamanan

- **Confidentiality** (Kerahasiaan): Email hanya boleh dilihat oleh orang yang menjadi tujuannya.
- **Integrity** (Integritas): Konten asli harus diterima oleh penerima tanpa perubahan.
- **Availability** (Ketersediaan): Penerima harus dapat mengakses email kapan saja saat dibutuhkan.

Transmisi Aman Email

- **Pretty Good Privacy (PGP)**
- **Secure/Multipurpose Internet Mail Extensions (S/MIME)**

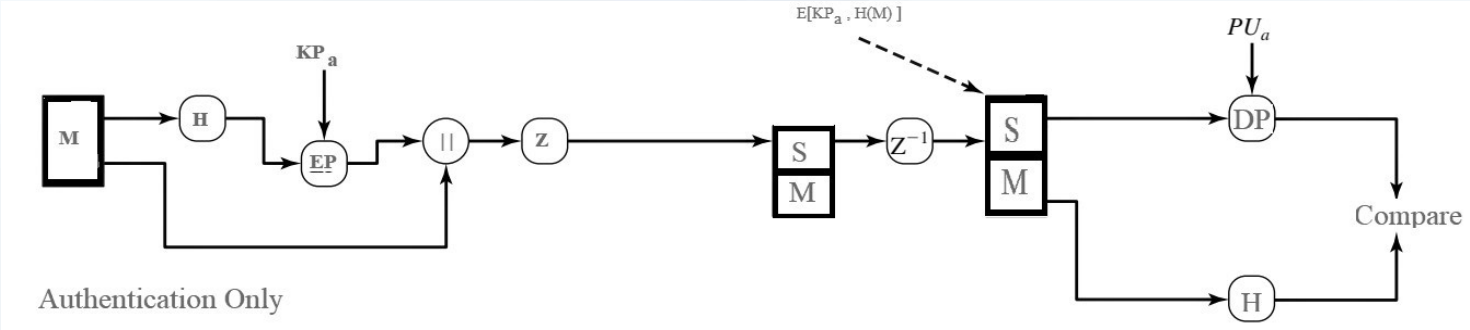
Pretty Good Privacy (PGP)

- Dikembangkan oleh **Phil Zimmermann** pada tahun 1991.
- Ada beberapa alasan yang dapat disebutkan untuk popularitasnya:
  - Tersedia secara gratis di seluruh dunia
  - Berdasarkan algoritma yang aman
  - Memiliki beragam penerapan

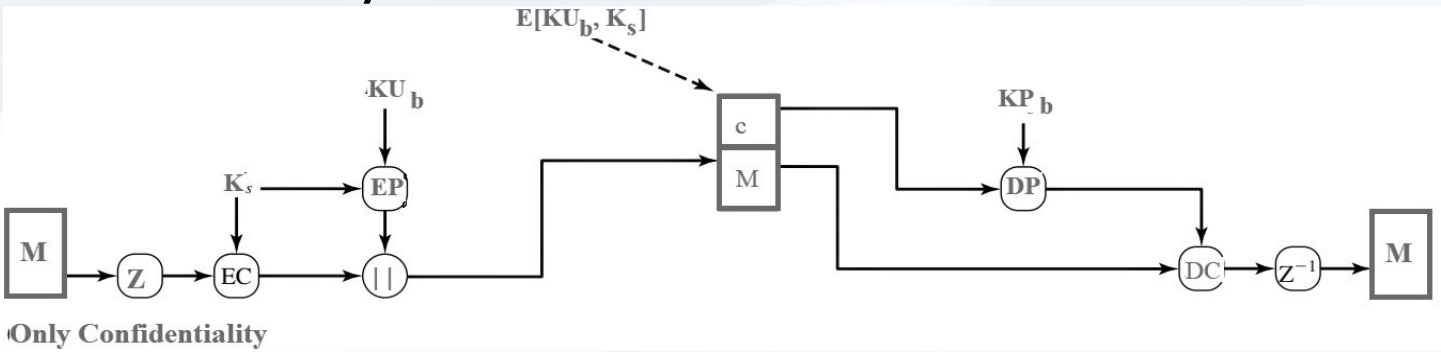
Deskripsi Operasional

- Matematika di balik PGP (Pretty Good Privacy) bisa menjadi cukup kompleks dalam langkah-langkahnya:
  - Authentication
  - Confidentiality
  - Compression
  - Email Compatibility
  - Segmentation

Authentication



Confidentiality



Secara praktis, layanan Autentikasi dan Kerahasiaan disediakan secara paralel.

Compression

Secara default, PGP melakukan kompresi setelah penandatanganan dan sebelum enkripsi.

- Menggunakan algoritma kompresi ZIP

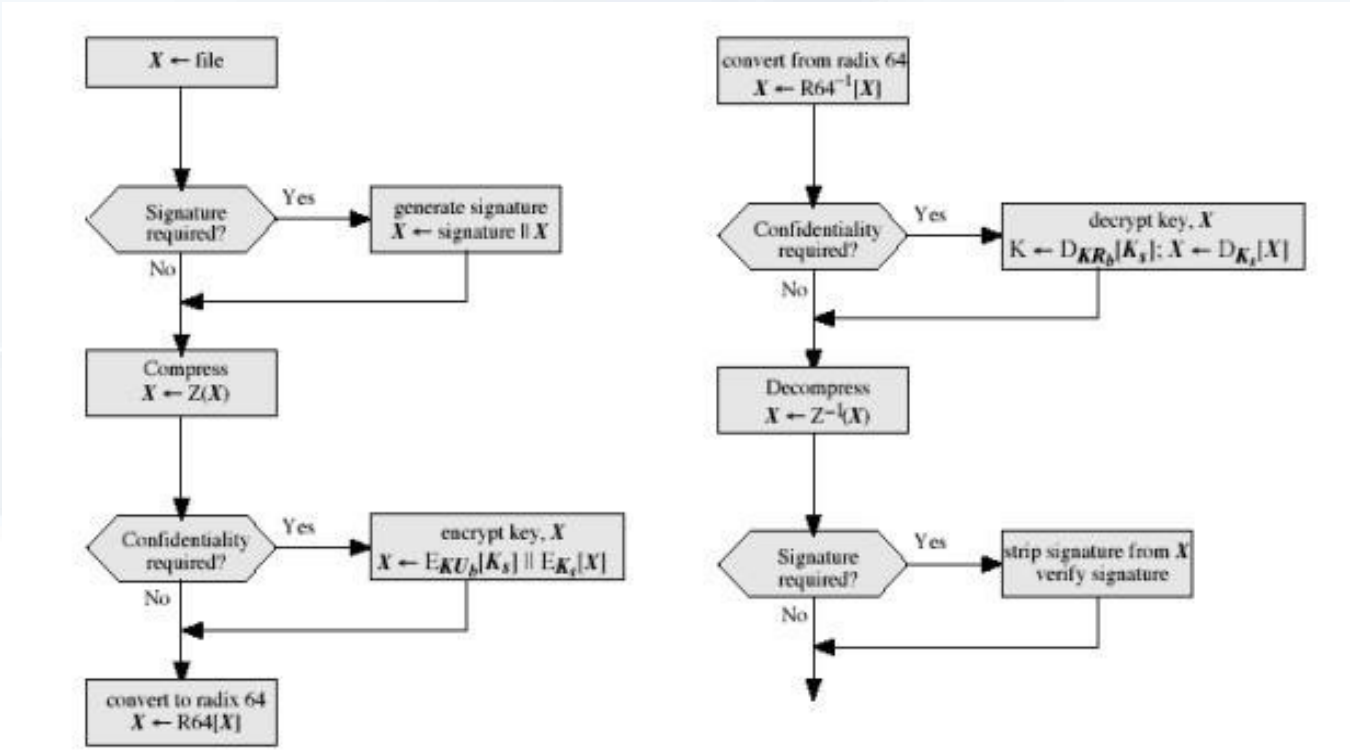
Email Compatibility

- PGP akan memiliki data biner untuk dikirim (pesan yang telah dienkripsi).
- Mengonversi aliran biner 8-bit mentah menjadi aliran karakter ASCII yang dapat dicetak untuk pengiriman.
- Menggunakan algoritma radix-64 untuk konversi.

Segmentation / Reassembly

- Protokol email bahkan dibatasi oleh panjang maksimum.
- PGP secara otomatis membagi pesan yang terlalu besar menjadi segmen-segmen yang cukup kecil untuk dikirim melalui email.
- Teknik "Divide and conquer" (Bagi dan taklukkan).
- Penyusunan kembali di sisi penerima diperlukan sebelum memverifikasi tanda tangan dan dekripsi.

Ringkasan PGP



Encryption sender side

Decryption receiver side

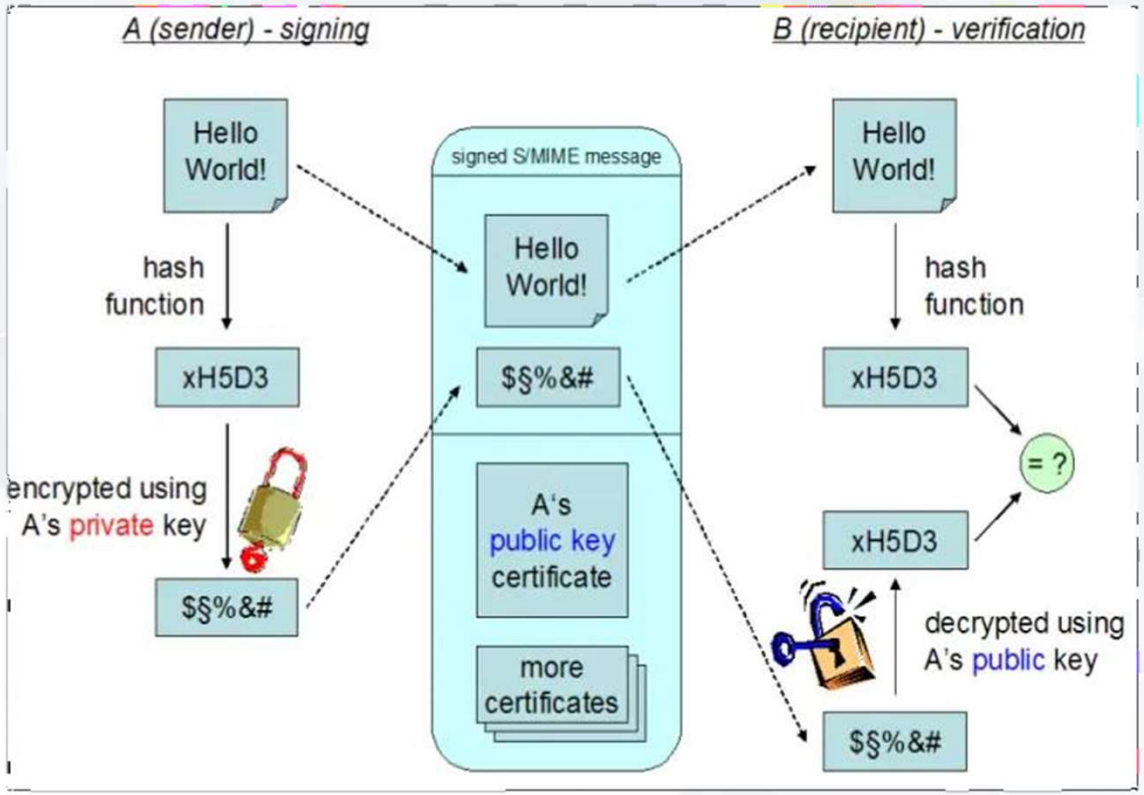
Secure/Multipurpose Internet Mail Extension (S/MIME)

- Awalnya dikembangkan oleh RSA Data Security
- Peningkatan keamanan pada data MIME yang dikirim melalui email
- MIME menggantikan protokol SMTP yang terbatas, karena SMTP tidak dapat menukar file multimedia.
- Didukung oleh program email utama seperti Outlook, Netscape

S/MIME Functions

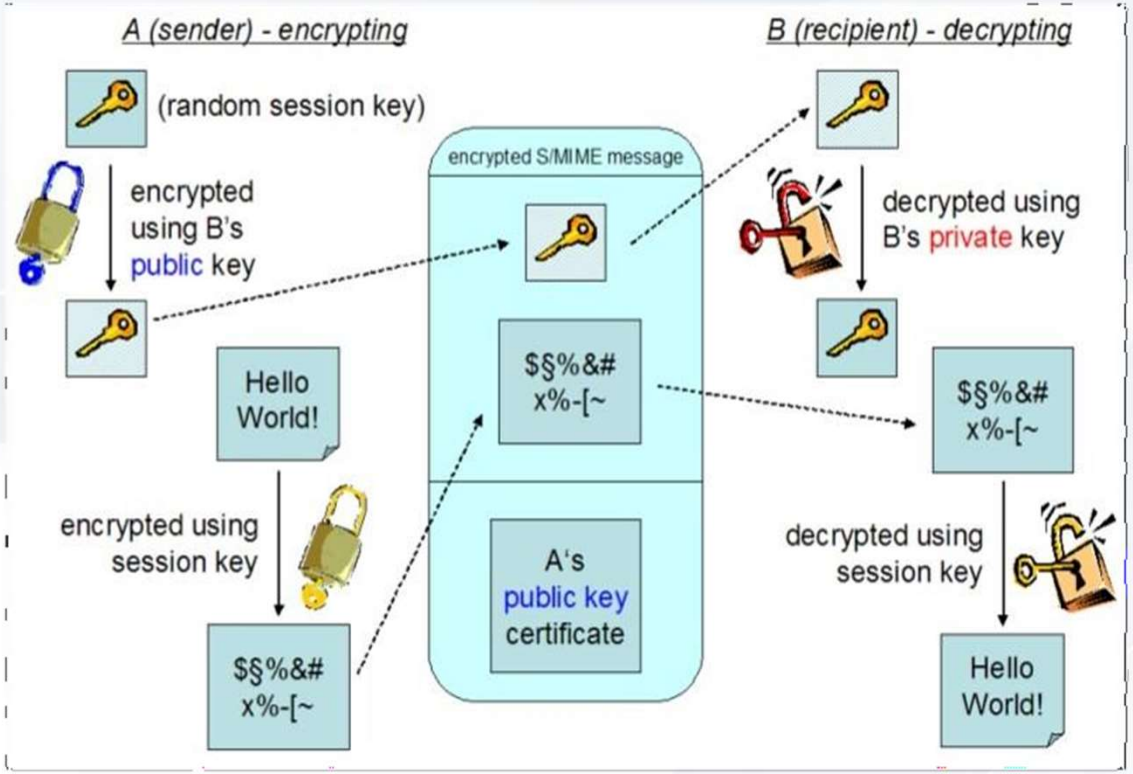
- **Enveloped data** (Data tertutup): konten yang dienkripsi & kunci terkait
- **Signed data** (Data yang ditandatangani): konten ditambah tanda tangan kemudian dikodekan menggunakan encoding base64
- **Clear-signed data** (Data tanda tangan jelas): hanya tanda tangan digital yang dikodekan menggunakan base64
- **Signed and enveloped data** (Data yang ditandatangani dan tertutup): entitas yang hanya ditandatangani dan hanya dienkripsi dapat disusun secara bersarang

S/MIME: Signed mail



Buatlah *message digest* yang akan digunakan untuk membentuk tanda tangan digital. Enkripsilah *message digest* untuk membentuk tanda tangan digital.

S/MIME: Encrypted Mail



- Enkripsilah kunci sesi untuk dikirim bersama pesan.
- Enkripsilah pesan untuk dikirim menggunakan kunci sesi sekali pakai.

Kesimpulan

- **Keamanan email** semakin penting seiring berjalannya waktu. Perusahaan menggunakannya untuk bertukar informasi penting.
- Penting untuk melindungi informasi ini. Jika peretas mendapatkan akses ke informasi ini, mereka dapat menjualnya kepada pesaing Anda. Dengan demikian, pesaing Anda akan mendapatkan keuntungan yang tidak adil. Penting untuk memastikan bahwa email Anda dienkripsi. Anda dapat menggunakan perangkat lunak enkripsi email untuk mengenkripsi email Anda. Ini akan memastikan bahwa hanya penerima Anda yang dapat mengakses email Anda.

Referensi

- E-mail Security: An Overview of Threats and Safeguards (ahima.org)
- https://en.wikipedia.org/w/index.php?title=Pretty_Good_Privacy&oldid=1028032091
- http://netaccess.on.ca/~rbarclay/bg2pgp.txt
- S/MIME Functionality and Messages (brainkart.com)
- rfc5751 (ietf.org)

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI

Kampus Merdeka INDONESIA JAYA

Single Degree Program

S2 - Sistem Informasi (M.Kom.)
S1 - Sistem Komputer (S.Kom.)
S1 - Sistem Informasi (S.Kom.)
S1 - Teknologi Informasi (S.Kom.)
S1 - Bisnis Digital (S.Bns.)
D3 - Manajemen Informatika (A.Md.Kom.)

Dual Degree International Program

S1 - Sistem Informasi (S.Kom., B.IT.)
(collaboration with HELP University)
S1 - Bisnis Digital (S.Bns., B.M.)
(collaboration with DNUI University)

Dual Degree National Program

S1 - Sistem Informasi (S.Kom., S.Ds.)
(collaboration with Universitas Teknologi Bandung)

www.stikom-bali.ac.id info@stikom-bali.ac.id (0361) 244445

STIKOMERS TV STIKOM Bali @stikombali

Always The First